APPENDIX

B

HANDS-ON EXERCISES

CHAPTER 1 KEY TERMS

Active Directory (AD) — Microsoft's new directory service. Active Directory stores information about network resources and allows users to search for and access those resources.

Active Directory Schema — Defines which objects can be stored in Active Directory and what attributes are associated with those objects. The Active Directory schema can be modified. This process is known as extending the schema.

Active Directory Services Interface (ADSI) — A programming interface that allows developers to access and control Active Directory.

attributes — Every object in Active Directory has one or more properties. These properties are known as the object's attributes.

Backup Domain Controller (BDC) — These Windows NT domain controllers are used for fault tolerance (in case the PDC goes offline) and for load balancing (to allow users to log in to the network through multiple systems). The BDC contains a read-only version of the database and cannot modify the objects contained within the database.

directory — A collection of data that is related to other pieces of data. Also known as a database.

domain — A logical collection of users and computers that share a common security profile.

domain controller (DC) — In Windows 2000, the PDC/BDC model no longer exists. Instead, the systems that control Active Directory are known simply as domain controllers. Each DC has a read/write version of the database and uses multimaster replication to replicate data.

Domain Name Service (DNS) — The naming system used for naming Active Directory domains. DNS is also the naming system used for the Internet, allowing for an easy transition between internal networks and the Internet.

Encrypted File System (EFS) — Allows users to lock down and encrypt files and folders on their system so that others cannot read them.

Group Policy — A new feature that allows you to secure and maintain Windows 2000 systems.

Internet Connection Sharing (ICS) — A technology that allows multiple computers in an organization to use a single connection to the Internet. All requests to and from the Internet are routed through the system running ICS.

Internet Information Server (IIS) — A built-in Web server that supports Active Server Pages. A new feature that allows you to control the amount of processing time a Web site receives, which is known as process throttling.

Lightweight Directory Access Protocol (LDAP) — An industry standard protocol for accessing directory information. Microsoft used LDAP as the main communication protocol for Active Directory.

metadata — The properties of an object are also known as the metadata of the object.

Microsoft Management Console (MMC) — A fully customizable tool for performing many of the Windows 2000 Administrative tasks. MMC uses snap-ins for each administrative tool and gives the administrator a common interface to work with.

mixed mode — When both Windows 2000 and Windows NT domain controllers exist, the network is said to run in mixed mode.

native mode — When all systems on the network are Windows 2000 and use Active Directory for authentication and lookup, the network is said to run in native mode. Once the mode is changed from mixed to native, it cannot be reversed.

network operating system — An operating system designed for file, print, and application sharing. These operating systems are optimized for server-based tasks.

nontransitive trust — One of the trust relationships used in Windows NT. In a nontransitive trust, trust relationships are not inherited. For example, if Domain A trusts Domain B, and Domain B trusts Domain C, then Domain A will not trust Domain C.

objects — Every resource that exists in Active Directory (user, group, computer, share, printer, etc.) is known as an object.

Organizational Unit — A container in Active Directory for grouping Active Directory objects that require similar configuration. Departments (Payroll or HR) and locations (Seattle or New York) are common divisions for defining organizational units.

Primary Domain Controller (PDC) — A Windows NT server that controls the directory (the user and group information). This is the only server that can modify any of the objects stored within the database. It will then replicate changes to the Backup Domain Controllers.

Remote Installation Services (RIS) — RIS is a service that simplifies the initial installation of Windows 2000 Professional systems. It uses the Pre-Boot Execution Environment (PXE) read-only ROM chip to connect the system to the RIS server. The operating system is then automatically installed.

replication — The process of sharing any changes to Active Directory objects between the domain controllers.

total cost of ownership (TCO) — A term describing the amount of money a product costs to purchase, implement, and support.

transitive trust — A trust in which multiple trusts are inherited by other trusts. For example, if Domain A trusts Domain B, and Domain B trusts Domain C, then Domain A will trust Domain C.

trust — A relationship that is set up between two domains, allowing the users from one domain to access the resources in the other.

Windows 2000 Advanced Server — Microsoft's enterprise version of Windows 2000 Server. It includes all the options available in Windows 2000 Server but includes scalability options such as network load balance and clustering.

Windows 2000 Datacenter Server — Microsoft's most advanced and powerful NOS in the Windows 2000 server family. Designed for data-warehousing implementations, it supports a large amount of memory (64 GB) and up to 32 processors. This version of Windows 2000 is only available for purchase with the high-end server hardware.

Windows 2000 Professional — The Windows 2000 version designed for the business desktop. The replacement for Windows NT Workstation.

Windows 2000 Server — Microsoft's new entry-level network operating system. The replacement for Windows NT Server.

Windows Scripting Host (WSH) — A powerful scripting language that can be used to script many common and tedious administrative tasks.

Chapter 1 Review Questions

1. What is the main reason for using Active Directory?
   a. Keeping track of network resources and enabling users to access this data
   b. Keeping track of resource usage on the network
   c. Keeping track of user information, such as phone numbers
   d. None of the above
2. With Windows NT, Microsoft introduced the concepts of Profiles and Policies. What does Windows 2000 use to define settings on systems in the network?
   a. Kerberos
   b. Access Control Lists
   c. Discretionary Access Control Lists
   d. Group Policy
3. Which industry standard did Microsoft choose to use when they developed Active Directory for Windows 2000?
   a. LDAP
   b. SMTP
   c. POP3
   d. IMAP4

4. A new feature in Windows 2000 allows for multiple computers to share the same Internet connection. What is the name of that feature?
   a. Internet Proxy
   b. Internet Line Sharing
   c. Shared Internet Connection
   d. Internet Connection Sharing
5. With Windows NT, Microsoft used the NetBIOS naming convention to keep track of systems and resolve their names to addresses. Which naming convention did Microsoft use with Windows 2000?
   a. NetBEUI
   b. NetBIOS
   c. DNS
   d. WINS
6. With Windows NT, all domain information was stored on all domain controllers, but only the Primary Domain Controller maintained the read/write version of the database. This information was then replicated to all the Backup Domain Controllers. If the PDC were to go offline, changes could not be made on the BDCs. This has changed in Windows 2000 because of which of the following?
   a. Multimaster authentication
   b. Multimaster replication
   c. Multimaster controllers
   d. Multimaster database
7. Active Directory requires that which of the following be installed, in order to function?
   a. WINS
   b. DHCP
   c. DNS
   d. NIS
8. A new feature in Windows 2000 allows users to protect their documents from being read. This is done using which feature?
   a. Disk Encryption System
   b. Encrypted Disk System
   c. File Encryption System
   d. Encrypted File System

9. Windows 2000 Professional supports up to four processors out of the box. True or False?

   a. True

   b. False

10. When Active Directory is installed in a Windows 2000 domain, the domain controllers (DCs) can operate in one of two modes. When only Windows 2000 systems are present, which mode does Microsoft recommend that you use?

    a. W2K mode

    b. WinNT mode

    c. Native mode

    d. Mixed mode

11. Many organizations currently use drive-mirroring technologies such as Ghost and DriveCopy to simplify workstation deployment and failure recovery. Microsoft included a feature in Windows 2000 that allows you to rapidly deploy Windows 2000 Professional on network systems. What is that new feature?

    a. Remote Installation Services

    b. Remote Boot Services

    c. Remote Imaging Services

    d. Remote Storage Services

12. Which Windows 2000 version or versions support disk quotas?

    a. Professional

    b. Server

    c. Advanced Server

    d. Datacenter Server

13. Which version or versions of Windows 2000 support up to 32 processors?

    a. Professional

    b. Server

    c. Advanced Server

    d. Datacenter Server

14. Which version of Windows 2000 is a replacement for Windows NT Workstation?

    a. Professional

    b. Server

    c. Advanced Server

    d. Datacenter Server

15. Which version or versions of Windows 2000 is/are a replacement for Windows NT Enterprise Edition?
    a. Professional
    b. Server
    c. Advanced Server
    d. Datacenter Server
16. When Active Directory is installed in a Windows 2000 domain, the domain controllers (DCs) can operate in one of two modes. When both Windows 2000 and Windows NT systems are present, which mode does Microsoft recommend that you use?
    a. W2K mode
    b. WinNT mode
    c. Native mode
    d. Mixed mode
17. Which version of Windows 2000 is the replacement for Windows NT Server – Terminal Server Edition?
    a. Professional
    b. Server
    c. Advanced Server
    d. Datacenter Server
18. Which version of Windows 2000 is a replacement for Windows NT Server?
    a. Professional
    b. Server
    c. Advanced Server
    d. Datacenter Server
19. Which feature of Windows 2000 makes adding components to the computer easier than in Windows NT?
    a. Plug and Play
    b. Windows 95/98 and Windows NT drivers work with Windows 2000.
    c. Windows 2000 uses generic drivers that work with all components.
    d. Microsoft introduced a law forcing all manufacturers to create drivers for Windows 2000.

20. Active Directory can store a predefined set of properties for objects and object attributes. What is this called?
    a. The Active Directory list
    b. The Active Directory directory
    c. The Active Directory database
    d. The Active Directory schema

Chapter 1 Case Projects

Case Project 1-1

Your organization would like to purchase a single system with 32 processors and have the processors and memory assigned to individual departments with no overlap. Which version of Windows 2000 does your organization need?

Case Project 1-2

A client of yours would like to implement a Windows 2000 cluster. Which Windows 2000 solution would you recommend?

Case Project 1-3

You are about to install Active Directory into your network. Which naming convention protocol needs to be installed and set up before the installation can be completed?

Chapter 2 Key Terms

classes — Collections of similar objects in Active Directory. Also known as Metadata.

container — An Active Directory object that can contain other objects, such as a domain or organizational unit.

domain naming master — The domain naming master controls the addition or removal of domains from the forest. Only a single domain naming master can exist for each forest.

Dynamic Domain Name Service (DDNS) — A new version of DNS that is used with Windows 2000. DDNS allows computers running the Windows 2000 operating system to register themselves to the DDNS service and deregister themselves from it.

forest — A collection of trees.

Global Catalog (GC) — A special limited database that stores partial replicas of all the directories of other domains. This allows users from a domain to become aware of resources on other domains without the need for full replication between all domains. By default, the first domain controller installed in the domain becomes the Global Catalog. Additional Global Catalogs can be configured manually.

hostname — The leftmost portion of a fully qualified domain name. This is the actual name of the system as it is accessed on the local network. For example, for the system with the mail.Austin.TexasPinball.com FQDN, the hostname is mail.

infrastructure master — The infrastructure master is responsible for maintaining all interdomain object references. It informs certain objects that other objects have been moved, changed, or modified. Only one infrastructure master can exist within a single domain.

intersite replication — Replication between sites.

intrasite replication — Replication within a site.

Knowledge Consistency Checker (KCC) — A service that generates the replication topology between and among sites.

namespace — A namespace defines the boundaries within a domain name. Any hosts and subdomains within the domain name are known to be part of the domain's namespace.

operations master — Several types of operations in Windows 2000 networks are impractical for multimaster environments. Windows 2000 uses a single DC to make these types of changes. That DC is known as the operations master.

PDC emulator — This operations master is used whenever non-Windows NT systems exist on the network. It acts as a Windows NT PDC for downlevel clients and for Windows NT BDCs. It accepts all password changes and replicates those changes into Active Directory. One PDC emulator can exist within each domain.

relative ID master — The relative ID (RID) master controls the sequence number for the DCs within the domain. The RID is used to recognize each DC in the domain as a DC. One RID master must exist within each domain.

schema master — The schema master controls all the updates and modifications to the schema within the domain. Only a single schema master can exist for each forest.

site — A site is a collection of computers connected via a high-speed network.

subdomain — If the domain name is stripped out of the fully qualified domain name, and more than just the hostname remains, then the portion immediately to the left of the domain name is known as a subdomain. For example, for the system with the mail.Austin.TexasPinball.com FQDN, the subdomain is Austin.

tree — A collection of domains that share a common schema, Global Catalog, and namespace.

Chapter 2 Review Questions

1. What naming resolution is used by default in Windows 2000?
    a. WINS
    b. NIS
    c. DHCP
    d. DNS

2. What is the definition of a domain?
   a. A collection of computers sharing the same operating system
   b. A collection of computers sharing the same resources
   c. A collection of computer, users, and other objects that share the same security boundary
   d. A physical collection of computers
3. What are Organizational Units used for?
   a. Subdivide a domain along administrative boundaries
   b. Define a new security boundary for the domain
   c. Subdivide a domain along geographical boundaries
   d. Create a relationship between two or more forests
4. What is the special version of DNS in Windows 2000 called?
   a. Double DNS
   b. Dynamic DNS
   c. Automatic DNS
   d. Proxy DNS
5. Which operations master communicates with non-Windows 2000 systems for authentication and logon?
   a. Schema master
   b. Domain naming master
   c. Relative ID master
   d. PDC emulator
   e. Infrastructure master
6. Which operation master controls all changes made to the Active Directory schema?
   a. Schema master
   b. Domain naming master
   c. Relative ID master
   d. PDC emulator
   e. Infrastructure master
7. Which operations master maintains all interdomain object references?
   a. Schema master
   b. Domain naming master
   c. Relative ID master
   d. PDC emulator
   e. Infrastructure master

8. Which operations master assigns RIDs to domain controllers in the domain?
   a. Schema master
   b. Domain naming master
   c. Relative ID master
   d. PDC emulator
   e. Infrastructure master
9. Which operations master controls the addition and removal of domains to and from the forest?
   a. Schema master
   b. Domain naming master
   c. Relative ID master
   d. PDC emulator
   e. Infrastructure master
10. Active Directory domains share which of the following characteristics when they exist within the same tree?
    a. Global catalog
    b. Schema
    c. Namespace
    d. All of the above
11. Schema objects and attributes can be deleted from the Active Directory Schema. True or False?
    a. True
    b. False
12. What type of server must exist in a mixed-mode domain to perform the logon process for Windows NT systems?
    a. Global Catalog
    b. PDC emulator
    c. DC
    d. BDC
13. Which operation master or masters can have only one instance per domain?
    a. Schema master
    b. Domain naming master
    c. Relative ID master
    d. PDC emulator
    e. Infrastructure master

14. Which operation master or masters can have only one instance per tree?
    a. Schema master
    b. Domain naming master
    c. Relative ID master
    d. PDC emulator
    e. Infrastructure master
15. What is the definition of a site?
    a. A site is a logical collection of computers sharing the same security boundary.
    b. A site is a physical collection of computers sharing the same security boundary.
    c. A site is a collection of computers connected via a high-speed network.
    d. A site is a geographical collection of computers.
16. Which Active Directory item has attributes associated with it?
    a. A class
    b. An attribute
    c. An object
    d. A user
17. What Windows 2000 component controls the replication topology between and among sites?
    a. Topology Master
    b. Knowledge Consistency Checker
    c. Topology Consistency Checker
    d. Knowledge Master
18. Replication between sites uses a preferred server to transmit the replication information through a single DC. What is this preferred server known as?
    a. Gateway server
    b. Proxy server
    c. Preferred server
    d. Bridgehead server
19. In the fully qualified domain name Mail1.Dallas.Texas.TexasPinBall.com, which is the hostname of the server?
    a. Mail1
    b. Mail1.Dallas
    c. Dallas.Texas
    d. TexasPinBall.com

CHAPTER 2 HANDS-ON PROJECTS

Project 2-1

1. Open the Active Directory Sites and Services MMC Snap-in by choosing **Start** | **Programs** | **Administrative Tools** | **Active Directory Sites and Services**.
2. Click the **Sites** folder under Active Directory Sites and Services if necessary. Choose the **New Site** option from the Action drop-down list.
3. In the New Object – Site Screen text box, enter a name for the remote site.
4. Select the site link for the site and click **OK**. Click **OK** in message saying site has been created.
5. Add the IP subnets to the site.
6. Install a DC into the site.
7. Close the AD Sites and Services console.

Project 2-2

1. Open the Active Directory Sites and Services MMC Snap-in by choosing **Start** | **Programs** | **Administrative Tools** | **Active Directory Sites and Services**.
2. Open the **Inter-Site Transports** folder.
3. Right-click on the appropriate transport protocol and choose the new site link from the drop-down menu.
4. Give the site link a name in the Name dialog box of the New Object – Site Link window.
5. Select the linked sites from the left column in the dialog box and click **Add** to associate them with the link.
6. Click **OK** to complete the site link creation process.
7. Close the AD Sites and Services console.

CHAPTER 2 CASE PROJECT

Case Project 2-1

You are migrating your network from Windows NT to Windows 2000. You install Windows 2000 and Active Directory and upgrade the PDC, but you find that Windows NT systems can no longer authenticate with it. You check to make sure that the network is running in mixed mode, which it is. What could be causing this lack of connectivity with the Windows NT systems?

Chapter 3 Key Terms

administrative OU model — An OU model based on the administrative structure within the organization.

administrative overhead — The amount of administrative resources (such as systems and people) required to perform administrative tasks.

business unit OU model — An OU model based on the business units within the organization. Similar to the administrative OU model, but on a much higher level.

departmental OU model — An OU model based on the organizational departments within the company, for example: Payroll, Engineering, HR, Public Relations, etc.

geographic OU model — An OU model based on the geographic layout of the organization. This model can take the form of different locations within a city, within a state, within the country, and within the world.

object OU model — An OU model that sees a different OU for every type of object within the domain, for example: users, groups, and printers.

replication overhead — The amount of network and system resources used for replication of information between domain controllers.

replication window — The period of time a site link is available for replication purposes.

Chapter 3 Review Questions

1. Which description defines a site in Active Directory?
   a. Any location that includes one or more domain controllers
   b. Any physical geographic location
   c. Any group of computers connected by a high-speed connection
   d. Any group of computers connected by a low-speed connection
2. Why would a domain controller not be placed at a specific location?
   a. Replication overhead
   b. Administrative overhead
   c. Hardware costs
   d. All of the above
3. What is the definition of a replication window?
   a. The period of time a site link is available for replication purposes
   b. The amount of data that can be replicated over a site link in a specified period of time
   c. The period of time a domain controller is available for replication purposes
   d. The amount of data that can be replicated by a domain controller in a specified period of time

4. Which of the following is NOT a reason for installing a DC in a specific location?
   a. High bandwidth connection to the other sites
   b. Low bandwidth connection to the other sites
   c. To speed authentication
   d. A domain is limited to just one site.
5. A Windows 2000 Active Directory site requires a domain controller to function. True or False?
   a. True
   b. False
6. Which OU model divides Active Directory objects by object type?
   a. Administrative model
   b. Business unit model
   c. Departmental model
   d. Geographic model
   e. Object model
7. Which OU model divides Active Directory by physical location?
   a. Administrative model
   b. Business unit model
   c. Departmental model
   d. Geographic model
   e. Object model
8. Which OU model divides Active Directory by department?
   a. Administrative model
   b. Business unit model
   c. Departmental model
   d. Geographic model
   e. Object model
9. Which OU model divides Active Directory according to the organization's administrative structure?
   a. Administrative model
   b. Business unit model
   c. Departmental model
   d. Geographic model
   e. Object model

10. Which OU model divides Active Directory by the organization's specific business groups?
    a. Administrative model
    b. Business unit model
    c. Departmental model
    d. Geographic model
    e. Object model
11. What is the definition of an Organizational Unit?
    a. A container object spanning a single forest
    b. A container object spanning multiple domains
    c. A container object spanning multiple domain trees
    d. A container object within a single domain
12. Domain groups rather than OUs are used to grant administrative control to Active Directory objects. True or False?
    a. True
    b. False
13. Under normal operating conditions, when compared to a Windows NT network, what does a Windows 2000 network require?
    a. Same bandwidth
    b. Less bandwidth
    c. More bandwidth
    d. Impossible to determine
14. In Windows 2000, trust relationships are automatically created within a domain tree. True or False?
    a. True
    b. False
15. For a domain name to function on the Internet, with whom should it be registered?
    a. It does not need to be registered.
    b. The Internet Ruling Body, or IRB
    c. An ICAAN-accredited registrar
    d. Microsoft.net
16. Windows 2000 trust relationships are nontransitive, while Windows NT trust relationships are transitive. True or False?
    a. True
    b. False

17. If your organization is to be accessed from the Internet, then two different domain names (one internal and one external) must be used. True or False?

    a. True

    b. False

18. With Windows 2000 domains, logon names take on which of the following structures (assuming that the username is joe and the domain is domain.com)?

    a. joe

    b. joe@domain

    c. joe@domain.com

    d. joe.domain.com

19. When planning for a Windows 2000 infrastructure upgrade, what should the first step be?

    a. Draw out the current environment

    b. Lay out the AD sites

    c. Place the DC in the sites

    d. Schedule replication

20. Active Directory integrates closely with WINS. True or False?

    a. True

    b. False

Chapter 3 Case Project

Case Project 3-1

Your organization contains three geographic locations connected by 64K ISDN links. You decided to create three different sites, but users at the remote sites complain of slow authentication and access to AD information. What could be causing the problems?

Chapter 4 Key Terms

authoritative — The DNS server that has the primary role and can make changes to the zone is known as the authoritative for the zone.

caching-only DNS server — A caching-only server does not maintain a database of hostname to IP address resolutions. It simply resolves client resolution requests and caches that information.

flat namespace — A manual method for resolving names and addresses. The HOSTS file is a common example.

forward lookup query — A client resolution request to resolve a host name to its IP address. This query is sent to the primary DNS server.

forwarding DNS server — A server used to communicate with DNS servers outside the local zone.

full zone transfer — The process of transferring the entire DNS database from the primary server to the secondary server.

fully qualified domain name (FQDN) — The full name of the host, including the hostname, subdomain(s) (if any), and domain. For example, www.widgets.com.

hierarchical namespace — The namespace used in the Internet. It is divided into different domain and subdomain levels.

HOSTS file — A flat namespace file used for manual name resolution.

incremental zone transfer — The process of transferring only the changes in the DNS databases from the primary server to the secondary server.

name resolution — The process of resolving computer-used addresses with human-used names.

nslookup — An application for resolving hostname and IP addresses directly with the DNS server. Also used for troubleshooting purposes.

primary DNS server — The master DNS server for the specified zone. This is the only server that can make changes to the zone entries.

relative distinguished name — A name that is relative to the domain that it exists in. This is normally simply the hostname. For example, the relative distinguished name for www.widgets.com would be www.

reverse lookup query — A client resolution request to resolve a host's IP address to its hostname. This query is sent to the primary DNS server.

root server — A set of servers on the Internet that are the authoritative for the entire Internet DNS namespace.

secondary DNS server — This server (or servers) acts as a backup to the primary DNS server. This server is used as a failover if the primary DNS server cannot be contacted.

Time To Live (TTL) — The length of time a DNS server will cache the results of a query.

zone — A zone is a partitioned portion of the overall DNS namespace.

zone transfer — The process by which changes made on the primary DNS server are replicated to all the secondary DNS servers in the zone.

Chapter 4 Review Questions

1. What does DDNS stand for?

   a. Dynamic DNS

   b. Distributed DNS

   c. Database DNS

   d. Data DNS

2. Which type of resource creates a record for a name server?
   a. SOA
   b. NS
   c. A
   d. PTR
3. Which type of resource creates a record for a mail server?
   a. SOA
   b. PTR
   c. A
   d. MX
4. Which type of resource creates a record for an alias to a hostname?
   a. SOA
   b. CNAME
   c. PTR
   d. A
5. Which type of resource creates a record for a hostname?
   a. SOA
   b. CNAME
   c. PTR
   d. A
6. Which type of resource creates a record for an IP address?
   a. SOA
   b. CNAME
   c. PTR
   d. A
7. Which type of resource creates a service record for a service that exists on a system?
   a. SRV
   b. SVR
   c. A
   d. SOA
8. Your network uses the 192.168.7.0 network. What would be the correct format of the reverse lookup zone name?
   a. 192.168.7.in-addr.arpa
   b. 192.168.in-addr.arpa

c. 7.168.192.in-addr.arpa

d. 168.192.in-addr.arpa

9. Which utility is most commonly used for troubleshooting DNS problems?

a. Tracert

b. Nslookup

c. Dnscfg

d. Ping

10. Which type of zone maps hostnames to IP addresses?

a. Standard primary zone

b. Forward lookup zone

c. Reverse lookup zone

d. Active Directory-integrated zone

11. Which type of zone maps IP addresses to hostnames?

a. Standard primary zone

b. Forward lookup zone

c. Reverse lookup zone

d. Active Directory-integrated zone

12. Which SOA record entry is used by the secondary DNS server(s) to decide whether a zone transfer is required?

a. TTL

b. Retry

c. Refresh

d. Serial number

13. Which type of DNS server does not contain any zone databases?

a. Primary

b. Secondary

c. Forwarding

d. Caching-only

14. Which type of DNS server contains a copy of the zone, which it transfers from the zone master server?

a. Primary

b. Secondary

c. Forwarding

d. Caching-only

15. Which type of DNS server is the master server for the zone and contains the read/write version of the database?
    a. Primary
    b. Secondary
    c. Forwarding
    d. Caching-only
16. What was the original method of resolving names on the Internet?
    a. LMHOSTS file
    b. HOST files
    c. WINS
    d. DNS
17. Which of the following is a fully qualified domain name?
    a. Microsoft.com
    b. www.microsoft.com
    c. www.microsoft
    d. www
18. Which of the following is considered to be a top-level domain?
    a. com
    b. org
    c. edu
    d. All of the above
19. Which of the following clients does DDNS work with? (Choose all that apply.)
    a. Windows 98
    b. Windows NT
    c. Windows 2000
    d. All of the above
20. When testing a DNS server, which type of test queries the local server for the resolution?
    a. Simple query
    b. Iterative query
    c. Forward lookup query
    d. Reverse lookup query

CHAPTER 4 HANDS-ON PROJECTS

Project 4-1

1. Select **Start|Settings|Control Panel**.
2. Double-click the **Add/Remove Programs** applet.
3. Click **Add/Remove Windows Components**.
4. Select **Networking Services** and click **Details**.
5. Select the **Domain Name System (DNS)** option and click **OK**.
6. Click **Next**. If necessary, insert the Windows 2000 Server CD-ROM and then click **OK**.
7. Click **Finish**. Click **Close** in the Add/Remove Programs window and then close the Control Panel.

Project 4-2

1. Select **Start|Programs|Administrative Tools|DNS**.
2. Navigate to the server where the DNS server is to be configured, right-click the server, and choose the **Configure the server** option.
3. When the Wizard appears, click **Next**.You see the Root Server screen, which asks if this is the first DNS server on the network. Make your selection, then click **Next**.You see the Forward Lookup Zone screen, which asks if you'd like to create a Forward Lookup Zone. If you click **Yes**, continue with Step 4. If you choose **No**, skip to Step 8 to finish the wizard.
4. Select the Zone type and click **Next**.
5. Enter a name for the new zone and click **Next**.
6. Select the **Create a new file with this name** or **Use this existing file** option.
7. Enter a name for the file.You see the Reverse Lookup Zone screen, which asks if you'd like to create a Reverse Lookup Zone. If you click **Yes**, you need to select a zone type, and then identify the zone with a network ID or a name. Click **Next**, then repeat Steps 6 and 7.Then continue with Step 8. If you click **No**, skip to Step 8.
8. Click **Finish**.
9. Close the DNS console window.

Project 4-3

1. Select **Start|Programs|Administrative Tools|DNS**.
2. Navigate to the server where the DNS server is to be configured, right-click the server, and choose the **New Zone** option.

3. When the Wizard appears, click **Next**.
4. Select the Zone type and click **Next**.
5. Select either the **Forward** or **Reverse lookup zone** option and click **Next**.
6. Enter a name for the new zone and click **Next**. If necessary, enter the network ID for the new zone.
7. Select the **Create a new file with this name** or **Use this existing file** option.
8. Enter a name for the file and click **Next**.
9. Click **Finish**.
10. Close the DNS console window.

Project 4-4

1. Do not configure any zones.
2. Make sure that the root servers are configured (this should be done by default).

Project 4-5

1. Select **Start|Programs|Administrative Tools|DNS**.
2. Expand the selected server where the new Forward Lookup Zone is to be created. Highlight the **Forward Lookup Zones** container under the server.
3. Right-click on the container and choose the **New Zone** option.
4. When the Wizard appears, click **Next**.
5. Choose the zone type and click **Next**.
6. Enter the name of the new zone and click **Next**.
7. Select the **Create a new file with this name** or **Use this existing file** option.
8. Enter a name for the file and click **Next**.
9. Click **Finish**.
10. Close the DNS console.

Project 4-6

1. Select **Start|Programs|Administrative Tools|DNS**.
2. Highlight the server to be tested.
3. Right-click on the server and choose the **Properties** option.
4. Click on the **Monitoring** tab.
5. Choose the **A simple query against this DNS server** checkbox and click on **Test Now**. If the server passes the test, a PASS notice will appear in the Test Results box.

6. Choose the **A recursive query to other DNS servers** checkbox and click on **Test Now**. If the server passes the test, a PASS notice will appear in the Test Results box.
7. Click **OK** in the Properties page, then close the DNS console.

Chapter 4 Case Projects

Case Project 4-1

Your organization has six internal DNS servers for resolving intranet addresses. Management has decided that only one of the six DNS servers will be allowed to generate queries for Internet name resolutions through the company's firewall. What would you do to ensure that all of the remaining five servers could still resolve Internet addresses?

Case Project 4-2

Your company's only DNS server is configured on the Developer group's development server. The problem is that the development server tends to be rebooted fairly regularly, at which point Internet addresses cannot be resolved. You have been informed that the development server is to remain the primary DNS server, but the problem still needs to be solved. What is a possible solution?

Chapter 5 Key Terms

circular logging — The process of reusing a set of log files. As a log file fills to capacity, another one is used. When that one is filled, the first log file is overwritten. This does not allow for full recovery of an Active Directory database; noncircular logging is required.

context — The relationship of all domains in a Windows 2000 Active Directory domain tree.

Directory Services Restore Mode — The Directory Services Restore Mode is a safe-mode option that allows an administrator to restore the SYSVOL directory and AD database from a backup. This option is only available on domain controllers.

multi-master domain model — In a multi-master domain model, each DC is a peer. This allows for fault tolerance by allowing any DC to process changes and updates to the AD database.

NetBIOS domain name — A name given to the Active Directory domain to allow for functionality with previous versions of Windows NT.

noncircular logging — The process of creating a new log file when the old one fills up. This method keeps copies of all the transactions done to the database, allowing for up-to-the-minute recovery of the database.

ntds.dit — A Windows 2000 Jet database, which contains the values for the objects within the domain and the values for the domain forest.

systemroot directory — The systemroot directory is the directory where Windows NT is installed. By default, this directory is the \winnt directory.

shared system volume — A series of folders containing the logon scripts and policy objects for both the enterprise and the local domain. The shared system volume must exist on an NTFS 5 partition.

Chapter 5 Review Questions

1. What is the maximum number of objects AD can support?
   a. 1,000
   b. 10,000
   c. 100,000
   d. 1,000,000 +
2. Where is the shared system volume stored?
   a. *%systemroot%*\system32\SYSVOL
   b. *%systemroot%*\System\SYSVOL
   c. *%systemroot%*\SYSVOL
   d. *%systemroot%*\SharedSYSVOL
3. Where is the current ntds.dit file stored?
   a. *%systemroot%*\
   b. *%systemroot%*\NTDS\
   c. *%systemroot%*\System\
   d. *%systemroot%*\System32\
4. Where is the ntds.dit file used by dcpromo.exe stored?
   a. *%systemroot%*\
   b. *%systemroot%*\NTDS\
   c. *%systemroot%*\System\
   d. *%systemroot%*\System32\
5. Which program is used to install AD on a system and promote it to a domain controller?
   a. ADPromo.exe
   b. DCPromo.exe
   c. ADSetup.exe
   d. This cannot be done. Windows 2000 must be reinstalled in Domain Controller Mode.

6. What is the Directory Services Restore Mode used for?
    a. To promote a member server to a DC
    b. To demote a DC to a member server
    c. To restore AD from a backup
    d. To back up AD
7. By default, when AD is installed, the Windows 2000 domain is set to run in native mode. True or False?
    a. True
    b. False
8. Which of the following statements about the shared system volume is true?
    a. The shared system volume must be installed on any NTFS partition.
    b. The shared system volume must be installed on any FAT32 partition.
    c. The shared system volume must be installed on the boot partition.
    d. The shared system volume must be installed on an NTFS 5 partition.
9. If DNS is not installed when the Active Directory Installation Wizard is executed, then it will ask you if you would like DNS installed. True or False?
    a. True
    b. False
10. Which logging method allows for backup of all AD transactions?
    a. Circular logging enabled
    b. Circular logging disabled
    c. All logging options accomplish this.
    d. This is not possible with AD.
11. How would you recover from a lost Directory Services Restore Mode password?
    a. Use the passrec.exe utility.
    b. Delete the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DSRM\Password key.
    c. Reinstall Active Directory.
    d. This password cannot be recovered.
12. How would you change the AD logging to circular?
    a. Change the logging properties in the Active Directory snap-in.
    b. Reinstall AD and choose the Circular Logging check box.
    c. Edit the Registry and set the Registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\CircularLogging value to 0.

   d. Edit the Registry and set the Registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\ Parameters\CircularLogging value to 1.

13. What occurs if dcpromo.exe is executed on a system already configured as a domain controller?
   a. Nothing. The program fails.
   b. AD is reinstalled.
   c. AD is removed.
   d. The domain name can be changed.

14. Which of the following is true?
   a. Windows 2000 and AD use the shared-master domain model.
   b. Windows 2000 and AD use the multi-master domain model.
   c. Windows 2000 and AD use the no-master domain model.
   d. Windows 2000 and AD use the single-master domain model.

15. As in Windows NT, if a member server is to become a domain controller, the operating system must be reinstalled. True or False?
   a. True
   b. False

16. Which of the following replication methods does not occur when the domain is switched into native mode?
   a. NETLOGON continues to run.
   b. The domain uses AD multi-master replication.
   c. Windows NT DCs can no longer join the domain.
   d. All DCs can now perform directory updates.

Chapter 5 Hands-on Projects

Project 5-1

1. Select **Start|Run**.
2. In the Open field, type **dcpromo**, and click **OK**.
3. When the Wizard appears, click **Next**.
4. In the Domain Controller Type window, choose the **Domain controller for a new domain** option, and click **Next**.
5. In the Create Tree or Child Domain window, choose the **Create a new domain tree** option, and click **Next**.

6. If a message box appears saying that the DNS server cannot be contacted, click **OK**.
7. Choose the **Install and Configure DNS** option, then click **Next**.
8. Choose the **Default permissions for users and groups** option, then click **Next**.
9. Choose the **Create a new forest of domain trees** in the Create or Join Forest window, and click **Next**.
10. Enter the full DNS name of the new domain, and click **Next**.
11. Enter the NetBIOS name that is to be assigned to this domain, then click **Next**.
12. Select the locations where the database and log files are to be stored, and click **Next**.
13. Choose the location for the shared system volume and click **Next**.
14. In the Directory Services Restore Mode Administrator Password window, choose a password that is to be used when you need to restore your Active Directory information, and click **Next**.
15. A summary screen will appear, informing you of all the options you selected. Click **Next** to start the installation.
16. A progress indicator will appear. When the installation is complete, the Completing the Active Directory Installation Wizard window will appear. Click the **Finish** button.
17. A dialog box will appear, notifying you that the system must be rebooted for the changes to take effect. Click **Restart Now** to complete the installation.

Project 5-2

1. For this project the students should work in pairs, and this project should be executed on the second computer. Select **Start|Run**.
2. In the Open field, type **dcpromo**, and click **OK**.
3. When the Wizard appears, click **Next**. A message box will appear, saying that the Domain is a Global Catalog server, so you should make sure users can access other Global Catalog servers. Click **OK**.
4. The Remove Active Directory window will appear. Make sure that the This server is the last domain controller in the domain option is NOT selected, and click **Next**.
5. Enter an Administrator's password and confirm it. Click **Next**.
6. A summary screen will appear. Click **Next** to begin the domain controller demotion.
7. When the demotion is completed, click **Finish**.
8. A dialog box will appear, notifying you that the system must be rebooted for the changes to take effect. Click **Restart Now** to complete the installation.

Project 5-3

1. For this project the students should work in pairs, and this project should be executed on the second computer. Select **Start|Run**.
2. In the Open field, type **dcpromo**, and click **OK**.

3. When the Wizard appears, click **Next**. A message box will appear, saying that the Domain is a Global Catalog server, so you should make sure users can access other Global Catalog servers. Click **OK**.
4. The Remove Active Directory window will appear. Make sure that the This server is the last domain controller in the domain option is selected, and click **Next**. Supply a network username and then click **Next**.
5. Enter an Administrator's password and confirm it. Click **Next**.
6. A summary screen will appear. Click **Next** to begin the domain controller demotion.
7. When the demotion is completed, click **Finish**.
8. A dialog box will appear, notifying you that the system must be rebooted for the changes to take effect. Click **Restart Now** to complete the installation.

Project 5-4

1. Select **Start**|**Programs**|**Administrative Tools**|**Active Directory Domains and Trusts**.
2. Select the domain to be managed.
3. Right-click and choose the **Properties** option.
4. On the General tab, click the **Change Mode** button.
5. Click the **Yes** button to change the mode from Mixed to Native. Click **OK** in the Properties page, then click **OK** in the operation successful message.
6. Close the Active Directory Domains and Trusts console.

Chapter 5 Case Project

Case Project 5-1

You have finally been given the go ahead to install Windows 2000 AD on your network. You have planned out the installation, installed and configured DNS, and installed a domain controller. Some users are complaining that they cannot access the domain. You realize that those people are all running non-Windows 2000 systems. You verify that the NetBIOS domain name that you entered during the AD setup process is correct, but the users still cannot access the domain. What could be the cause of this problem, and what would be a solution to solve it?

Chapter 6 Key Terms

connection object — Windows 2000 DCs represent the inbound replication through this special object.

cost — A value given to a site link that defines the relative speed of the link in relation to the other links within the network.

DEFAULTIPSITELINK — The default site link created by Windows 2000 that is used to establish the replication process of the AD service.

domain naming master — The domain naming master controls the addition or removal of domains from the forest. Only a single domain naming master can exist for each forest.

Global Catalog (GC) — A special limited database that stores partial replicas of all the directories of other domains. This allows users from a domain to become aware of resources on other domains without the need for full replication among all domains. By default, the first domain controller installed in the domain becomes the Global Catalog. Additional Global Catalogs can be configured manually.

infrastructure master — The infrastructure master is responsible for maintaining all interdomain object references. It informs certain objects that other objects have been moved, changed, or modified. Only one infrastructure master can exist within a single domain.

intersite replication — Replication between sites.

intrasite replication — Replication within a site.

Knowledge Consistency Checker (KCC) — A service that generates the replication topology between and among sites.

operations master — Several types of operations in Windows 2000 networks are impractical for multi-master environments. Windows 2000 uses a single DC to make these types of changes. That DC is known as the operations master.

PDC emulator — This operations master is used whenever non-Windows NT systems exist on the network. It acts as a Windows NT PDC for downlevel clients and for Windows NT BDCs. It accepts all password changes and replicates those changes into Active Directory. One PDC emulator can exist within each domain.

relative ID master — The relative ID (RID) master controls the sequence number for the DCs within the domain. The RID is used to recognize each DC in the domain as a DC. One RID master must exist within each domain.

schema master — The schema master controls all the updates and modifications to the schema within the domain. Only a single schema master can exist for each forest.

site link — Sites are connected by site links. These site links are low bandwidth or unreliable/occasional connections between the sites.

transport — The type of transport used to replicate the directory information between the DCs. There are two different transports to choose from: synchronous RPC over a routed TCP/IP connection, or asynchronous Simple Mail Transfer Protocol (SMTP) connection over the underlying mail transport network.

Chapter 6 Review Questions

1. Which site is automatically created by Windows 2000 Active Directory?
   a. Default-Site
   b. First-Site

   c. First-Default-Site
   d. Default-First-Site
2. OUs are designed to contain only user and group objects. True or False?
   a. True
   b. False
3. Which administrative tool is used to administer the schema master?
   a. Active Directory Users and Computer
   b. Active Directory Domains and Trusts
   c. Active Directory Sites and Services
   d. Active Directory Schema Manager
4. Which administrative tool is used to administer the relative ID master?
   a. Active Directory Users and Computer
   b. Active Directory Domains and Trusts
   c. Active Directory Sites and Services
   d. Active Directory Schema Manager
5. Which administrative tool is used to administer the domain naming master?
   a. Active Directory Users and Computer
   b. Active Directory Domains and Trusts
   c. Active Directory Sites and Services
   d. Active Directory Schema Manager
6. Which administrative tool is used to administer the PDC emulator master?
   a. Active Directory Users and Computer
   b. Active Directory Domains and Trusts
   c. Active Directory Sites and Services
   d. Active Directory Schema Manager
7. Which administrative tool is used to administer the infrastructure master?
   a. Active Directory Users and Computer
   b. Active Directory Domains and Trusts
   c. Active Directory Sites and Services
   d. Active Directory Schema Manager
8. What is used to define explicit replication routing?
   a. Site link bridge
   b. Site trust relationship
   c. Domain link bridge
   d. Routing link bridge

9. What is the definition of a site in Windows 2000?
   a. A group of computers sharing the same security information
   b. A group of computers sharing the same IP subnet
   c. A group of computers connected by a low-speed connection
   d. A group of computers connected by a high-speed connection
10. Which administration utility is used to create and manage sites?
    a. Active Directory Users and Computer
    b. Active Directory Domains and Trusts
    c. Active Directory Sites and Services
    d. Active Directory Schema Manager
11. What is the main reasoning behind implementing sites?
    a. To set up security boundaries
    b. To set up a replication schedule
    c. To simplify administration
    d. To compress replication data
12. Manually created connection objects will remain in place until manually deleted. True or False?
    a. True
    b. False
13. The lower the site cost, the faster the site is deemed to be. True or False?
    a. True
    b. False
14. When a new site link is created, what is the default cost assigned to it?
    a. 0
    b. 1
    c. 50
    d. 100
15. When are site link bridges transitive?
    a. In a nonrouted network
    b. In a routed network
    c. All the time
    d. Never
16. Choose the two types of transports available for site links.
    a. SMTP
    b. ESMTP

c. IP

d. TCP

17. You can only have a single Global Catalog server in each domain. True or False?

a. True

b. False

18. Which transport does the DEFAULTIPSITELINK use?

a. Synchronous RPCs over SMTP

b. Synchronous RPCs over TCP/IP

c. Asynchronous SMTP

d. Asynchronous TCP/IP

19. OUs are created and managed using which utility?

a. Active Directory Users and Computer

b. Active Directory Domains and Trusts

c. Active Directory Sites and Services

d. Active Directory Schema Manager

20. Which utility is used to configure whether a server is a Global Catalog server?

a. Active Directory Users and Computer

b. Active Directory Domains and Trusts

c. Active Directory Sites and Services

d. Active Directory Schema Manager

CHAPTER 6 HANDS-ON PROJECTS

Project 6-1

1. Select **Start|Programs|Administrative Tools|Active Directory Sites and Services**.
2. Right-click on the **Sites** folder and choose the **New Site** option.
3. Enter a name for the new site. Select a site link object, and click **OK**.
4. Click **OK** to complete the site creation.
5. Close the AD Sites and Services console.

Project 6-2

1. Select **Start|Programs|Administrative Tools|Active Directory Sites and Services**.
2. Expand the Sites folder, right-click on **Subnets**, then choose the **New Subnet** option.

3. Enter the IP address for the network.
4. Enter the subnet mask for the network.
5. Choose the site to be associated with this subnet.
6. Click **OK** to create the subnet.
7. Close the AD Sites and Services console.

Project 6-3

1. Select **Start**|**Programs**|**Administrative Tools**|**Active Directory Sites and Services**.
2. Expand the Sites folder, then choose the **Inter-Site Transports** folder.
3. Choose the desired transport protocol. Right-click on the protocol and choose **New Site Link**.
4. Enter the name of the new link.
5. From the left pane, choose the sites that this link is to connect.
6. Click **Add** to add them to the site link.
7. Click **OK** to create the site link.
8. Close the AD Sites and Services console.

Project 6-4

1. Select **Start**|**Programs**|**Administrative Tools**|**Active Directory Sites and Services**.
2. Expand the Sites folder, then expand the **Default-First-Site-Name** folder.
3. Expand the **Servers** folder.
4. Choose the DC that is to be moved to the other site.
5. Right-click on the DC and choose the **Move** option.
6. Choose the Target site from the list.
7. Click **OK** to move the DC.
8. Close the AD Sites and Services console.

Project 6-5

1. Select **Start**|**Programs**|**Administrative Tools**|**Active Directory Sites and Services**.
2. Expand the Sites folder, then expand the site in which the server exists.
3. Expand the **Servers** folder.
4. Choose the server that is to become a GC server.
5. Choose the NTDS Settings in the right pane.

6. Right-click and choose **Properties**.
7. If necessary, check the **Global Catalog** option.
8. Click **OK** to configure the server as a GC server.
9. Close the AD Sites and Services console.

Project 6-6

1. Select **Start|Programs|Administrative Tools|Active Directory Sites and Services**.
2. Expand the Sites folder, then expand the **Inter-Site Transports** folder.
3. Choose the transport to be used for the site links.
4. Right-click and choose **Properties**.
5. Unselect the **Bridge all site links** option in the General tab.
6. Click **OK** to configure the site link bridge.
7. Close the AD Sites and Services console.

Chapter 6 Case Project

Case Project 6-1

Your organization is made up of two locations, HeadOffice and Sales. All the servers are installed in the HeadOffice location. The two locations are connected by slow links. Users at the Sales office complain about the speed of the network. What is the easiest way to alleviate some of the slow network issues?

Chapter 7 Key Terms

Access Control List (ACL) — A list of everyone who has been granted access to an object and the actions that users or groups can perform on those objects.

actions — Similar to permissions. Actions outline what users can do when they gain access to an object.

common objects — Objects that have been defined in the Active Directory schema. Examples are user accounts, contacts, groups, printers and shared folders.

delegation of control — The process of delegating some administrative tasks to different individuals.

extensible — The ability of developers and applications to create their own objects within Active Directory makes Active Directory extensible.

Globally Unique Identifier (GUID) — Similar to a SID, except that this ID is completely unique within the network.

inheritance — The ability for different containers and objects in Active Directory to inherit their permissions from their parent object. This simplifies the administration of permissions.

leaf object — An object with no objects contained within it.

LostAndFound container — A container used to stored orphaned objects.

orphaned object — Any child object whose parent object was either moved or no longer exists.

permissions — A set of rules used to control access to resources on the server and network.

publishing — The process of making Active Directory objects available for viewing.

security identifier (SID) — A unique ID given to every object in Active Directory. This SID is used to identify the object, and it allows objects with the same name to exist in the database.

special permissions — A completely customized set of permissions that can be assigned to a user or group.

standard permissions — A predetermined set of permissions that can be assigned to a user or group.

Chapter 7 Review Questions

1. Which utility is used to move member servers from one domain to another?
   a. MoveTree
   b. MoveServer
   c. NetDom
   d. Active Directory Users and Computers
2. Which application is used to grant administrative permissions to a user or group?
   a. Active Directory Users and Groups
   b. Active Directory Delegation Utility
   c. Delegation of Control Wizard
   d. Delegation of Permissions Wizard
3. Which property list contains user and group permissions for objects?
   a. Access Control List
   b. Access Control Group
   c. Access Control Permissions
   d. Access Control Rights
4. Which Identifier is unique within the entire forest?
   a. SID
   b. GUID

c. SUID

d. GID

5. Which utility is used to move objects between domains?

a. MoveObject

b. MoveParent

c. MoveChild

d. MoveTree

6. What sort of data should you not publish in Active Directory?

a. Static data (data that rarely changes)

b. Dynamic data (data that always changes)

c. Small amounts of data

d. Useful information

7. Which of the following are standard permissions?

a. Read

b. Change

c. Delete

d. Full Control

8. The Active Directory schema is not extensible. True or False?

a. True

b. False

9. Which options are available to you when you choose to disable the Allow Inheritable Permissions From Their Parent To Propagate To This Object option?

a. Copy

b. Remove

c. Modify

d. Cancel

10. Which of the following is not a common object in Active Directory?

a. User

b. Group

c. Conference room

d. Contact

11. What is the term for an object that does not contain other objects?

a. Standard object

b. Leaf object

c. Branch object

d. Child object

12. By default, which permission is granted to a newly created object?

a. Everyone: No Access

b. Everyone: Read

c. Everyone: Modify

d. Everyone: Full Control

13. Once the Active Directory schema is extended, the new objects and attributes can be deleted at any time. True or False?

a. True

b. False

14. You moved a container object from one domain to another. However, when you check the container object, you realize that the leaf objects within it were not moved. Where are they located?

a. In the root of the old domain

b. In the root of the new domain

c. In the LostAndFound container of the old domain

d. In the LostAndFound container of the new domain

15. Which of the following does an object in a Windows 2000 domain require?

a. Unique name

b. Unique description

c. Unique name and description

d. None of the above

CHAPTER 7 HANDS-ON PROJECTS

Hands-on Project

Project 7-1

1. Select **Start**|**Programs**|**Administrative Tools**|**Active Directory Users and Computers**.
2. Navigate to the container in which you would like the Windows NT printer created.
3. Right-click the container and choose the **New**|**Printer** option from the drop-down menu.
4. Enter the UNC name of the printer (for example, \\server\printer).
5. Click **OK** to create the printer.
6. Close the Active Directory Users and Computers console.

Project 7-2

1. Select **Start**|**Programs**|**Administrative Tools**|**Active Directory Users and Computers**.
2. Navigate to the container in which you would like to search for the Windows NT printer.
3. Right-click the container and choose the **Find** option.
4. In the Find list box, select **Printers**.
5. Enter the name of the printer in the Name field, and click **Find Now** to search for the printer.
6. Close the Active Directory Users and Computers console.

Project 7-3

1. Select **Start**|**Programs**|**Administrative Tools**|**Active Directory Users and Computers**.
2. Select the container in which you would like to create the user. Right-click the container, choose **New**|**User**.
3. Enter the desired information (such as first name, middle initial, last name, and user login name), and click **Next**.
4. Enter the user's password and confirm it. Choose any other options for this account (User must change password at next logon, User cannot change password, Password never expires, or Account is disabled). Click **Next**.
5. Click **Finish** to create the user.
6. Close the Active Directory Users and Computers console.

Project 7-4

1. Select **Start**|**Programs**|**Administrative Tools**|**Active Directory Users and Computers**.
2. Navigate to the container in which the user that you would like to enable resides. Click the user object to select it.
3. Right-click the selected user and choose the **Copy** option from the drop-down menu.
4. The Copy Object – User window appears. Enter the required information and click **Next**.
5. Enter the password (if any) and confirm it. Select any other desired options and click **Next**.
6. Click **Finish** to complete the user account copy.
7. Close the Active Directory Users and Computers console.

Project 7-5

1. Select **Start**|**Programs**|**Administrative Tools**|**Active Directory Users and Computers**.
2. Right-click the domain or container in which you would like to create the Organizational Unit, and choose the **New**|**Organizational Unit** option from the drop-down menu.
3. Enter the name of the new Organizational Unit.
4. Click **OK** to create the Organizational Unit.
5. Close the Active Directory Users and Computers console.

Project 7-6

1. Select **Start**|**Programs**|**Administrative Tools**|**Active Directory Users and Computers**.
2. Navigate to the domain in which the Organizational Unit resides.
3. Right-click the Organizational Unit and choose the **Delegate Control** option from the drop-down menu.
4. Click **Next**.
5. Click **Add**.
6. Select the desired users and/or groups, and click **Add**.
7. Click **OK**.
8. Click **Next**.
9. Choose the tasks that you would like to grant these users and/or groups permissions to perform.
10. Click **Next**.
11. Click **Finish**.
12. Close the Active Directory Users and Computers console.

Project 7-7

1. Select **Start**|**Programs**|**Administrative Tools**|**Active Directory Users and Computers**.
2. Navigate to the domain or container in which the Organizational Unit resides.
3. Right-click the Organizational Unit and choose the **Delete** option from the drop-down menu.
4. Click **Yes** to confirm the deletion of the Organizational Unit.
5. Close the Active Directory Users and Computers console.

Chapter 8 Key Terms

alerts — Alerts are used to configure the system to react to the status and state of different objects and object levels. For example, using alerts can generate system messages, start a log file, or start an application.

Application Log — The Application Log records events for applications that exist on the system. Not all applications write to the Application Log; they need to be developed to do so. The Application Log is useful for troubleshooting a failure of a specific application.

baseline — A measurement or snapshot of how the server will operate when things are running normally.

counter logs — Simple ways of creating templates for your performance-monitoring tasks.

counters — A counter is used to measure the various aspects of an object. For example, the Processor object has counters to measure Processor Time and Interrupts/Second.

Desktop Management Interface (DMI) — The predecessor to WMI. It allowed for a loose collection of generic function calls for gathering data from different systems.

Directory Service log — The Directory Service log is used to record all messages generated by Active Directory.

DNS Server log — The DNS Server log records all events that are generated by the Domain Name System (DNS) operations on a DC.

error event — This type of message records the failure of a component or application. An error event message usually means that something major has failed on the system.

File Replication Service log — The File Replication Service log records all messages with regards to the file replication process.

hard page fault — A hard page fault occurs when a process attempts to gain access to data that is not held in memory.

information event — This type of message records the successful operation of a task or application.

instances — Some systems have many duplicate objects. These are known as instances. Dual processor systems, for example, have two different Processor objects or two different Processor instances. Using the different instances allows the objects to be measured together or individually.

object — An object is a system resource. Objects can include the network interface, memory, processor, or hard disks. A System Monitor object is different from an Active Directory object.

paging — When a system is running low on physical memory, it writes out to the hard disk. This process is known as paging.

perfmon — A built-in tool for monitoring a Windows 2000 system. Also known as System Monitor.

queue — When a server or a component in a server begins to fall behind, some tasks have to wait before they are processed. The "line" in which these tasks wait to be processed is known as the queue.

response time — A measurement of elapsed time from the beginning of a process to its conclusion.

Security Log — The Security Log records successful and failed attempts at accessing objects and resources on the system. It responds to auditing events that are configured via the Computer Management MMC snap-in and Group Policy settings.

signature — Similar to a baseline but also includes the level of performance of a normal day.

System Log — The System Log is the location to which all messages generated by the system are stored.

System Monitor — A built-in tool for monitoring a Windows 2000 system. Also known as perfmon.

throughput — The number of processes and tasks that are done on the system within a given amount of time.

trace logs — Trace logs allow you to configure samples of data to be collected from providers on the system.

Update Sequence Numbers (USN) — A value replicated between systems to ensure that all the updated data is replicated between replication partners. Ensures that all the data is synchronized.

warning event — This type of message records a warning about an event that may or may not be significant, but that does not affect the operation of the component or application that has generated it.

Web-Based Management Instrumentation (WBEM) — Same as WMI. Microsoft decided to adopt the WBEM initiative, but named it WMI instead.

Windows Management Instrumentation (WMI) — A Microsoft standard for monitoring and collecting data from a wide range of computers running Windows 2000.

Chapter 8 Review Questions

1. Which tool is used to view the replication partners for a DC using the command line?
   a. REPADMIN
   b. REPLMGR
   c. Active Directory Replication Monitor
   d. Active Directory Replication Administrator
2. Which graphical tool is used to view the replication partners for a DC?
   a. REPADMIN
   b. REPLMGR

   c. Active Directory Replication Monitor

   d. Active Directory Replication Administrator

3. Which counter should you use to figure out if your system has run out of physical RAM and how much of the hard disk it's using to store information?

   a. % Paging

   b. Paging/Second

   c. % Usage

   d. Page Usage/Second

4. Which tool is used to read the logs on the local Windows 2000 system?

   a. System Monitor

   b. Event Logger

   c. Event Manager

   d. Event Viewer

5. Which tool is used to read the logs on a remote Windows 2000 system?

   a. System Monitor

   b. Event Logger

   c. Event Manager

   d. Event Viewer

6. Using System Monitor, what can you configure to page you, should the system processor exceed 95% utilization?

   a. Counter logs

   b. Alerts

   c. Trace logs

   d. Page logs

7. Which of the three events logs records an event that does not affect the system?

   a. Information

   b. Warning

   c. Error

8. Which of the three events logs records an event that does affect the system?

   a. Information

   b. Warning

   c. Error

9. Which of the three events logs records an event that could affect the system?

   a. Information

   b. Warning

   c. Error

10. When the system cannot keep up with all the different processes that request to be executed, the tasks are stored in a ______________.
    a. Queue
    b. Throughput
    c. Response time
    d. List
11. As mentioned, the Disk object statistics can be inaccurate when using which of the following server components?
    a. SCSI drives
    b. IDE drives
    c. SCSI controllers
    d. RAID 5 controllers
12. What is the definition of response time?
    a. The amount of time it takes the system to process the data
    b. The amount of time it takes a process to start
    c. The amount of time it takes a process to finish
    d. The amount of time it takes the process to execute
13. What is the definition of a queue?
    a. A group of processes that are waiting to be executed
    b. A group of processes that have been executed
    c. The amount of time it takes a process to execute
    d. The amount of data that is processed on the network
14. What is the definition of throughput?
    a. The amount of data that is processed by the system
    b. The amount of data that is processed by a service
    c. The amount of data that is processed in a specified amount of time
    d. The amount of data that is processed by an application
15. Which three components make up the data System Monitor can process?
    a. Processes
    b. Instances
    c. Objects
    d. Counters
16. Once you have configured a log with all of your desired objects, counters, and instances, you have the ability to save them collectively as what?
    a. Counter log
    b. Trace log

c. Alert log

d. Database log

17. You suspect that Exchange 2000 services are failing. Which event log would you search to find the Exchange 2000 logs?

    a. Application Log

    b. Security Log

    c. System Log

    d. Directory Service log

18. You suspect that a hacker is attempting to gain access to unauthorized systems and files on your network. You check the Security Log and find it empty. What is the most likely reason?

    a. The hacker has cleared the Security Log.

    b. The Security Log does not monitor access to files and systems, only to applications.

    c. A hacker is not attempting to access your systems.

    d. Auditing has not been turned on via the Computer Management MMC snap-in and Group Policy settings.

19. When the system runs out of physical memory and starts using the hard disk, it is ________________.

    a. Swapping

    b. Paging

    c. Queuing

    d. Mapping

20. What is the default maximum size for each of the event logs in Windows 2000?

    a. 256K

    b. 512K

    c. 1024K

    d. 2048K

Chapter 8 Hands-on Projects

Project 8-1

1. Select **Start|Programs|Administrative Tools|Performance**.
2. Right-click in the right pane, and choose the **Add Counter** option.
3. Choose a performance object.
4. Select the counters to monitor.

5. If multiple instances exist, choose the desired instance.
6. Click **Add** to add the counter.
7. Repeat for any other desired performance objects and counters.
8. Click Close to close the Add Counters dialog box.
9. Close the Performance console.

Project 8-2

1. Select **Start|Programs|Administrative Tools|Performance**.
2. In the left pane, select the **Performance Logs and Alerts|Counter Logs** container.
3. Right-click **Counter Logs** and choose the **New Log Settings** option.
4. Enter a name for the new counter log and click **OK**.
5. Click **Add** and choose the counter or counters that you would like added to the log, then click **Add** again, and then click **Close**.
6. Specify the logging interval by entering the number in the Interval field, and the units for the interval (seconds, minutes, hours, or days) in the Units field.
7. Click the **Log Files** tab.
8. Enter the log file information, including name, location, size, and type.
9. Click the **Schedule** tab.
10. Enter the start/stop information for the counter log.
11. Click **OK**.
12. Close the Performance console.

Project 8-3

1. Select **Start|Programs|Administrative Tools|Performance**.
2. In the left pane, select the **Performance Logs and Alerts|Trace Logs** container.
3. Right-click **Trace Logs** and choose the **New Log Settings** option.
4. Enter a name for the new trace log, and click **OK**.
5. To log system provider events, select the **Events logged by system provider** radio button and select the desired providers to be used for the trace log.
6. To log nonsystem providers, select the **Nonsystem providers** radio button.
7. Click **Add**, then select the providers, then click **OK**.
8. Click the **Log Files** tab.
9. Enter the log file information, including name, location, size, and type.
10. Click **Schedule** and enter the start/stop information for the trace log.

11. Click **OK**.
12. Close the Performance console.

Project 8-4

1. Select **Start**|**Programs**|**Administrative Tools**|**Performance**.
2. In the left pane, select the **Performance Logs and Alerts**|**Alerts** container.
3. Right-click in the right pane and choose the **New Alert Settings** option.
4. Enter a name for the new alert and click **OK**.
5. Optional: Enter a comment for the alert.
6. Click **Add**, select the desired counter, click **Add**, and click **Close**.
7. Select the counter.
8. To cause an alert when the counter is either over or under the limit, select the **Over** or **Under** option from the value drop-down list, and enter the limit in the Limit field.
9. Specify the logging interval by entering the number in the Interval field, and the units for the interval (seconds, minutes, hours, or days) in the Units field.
10. Select the **Action** tab.
11. To log an entry: Check the **Log an entry in the application event log** check box.
12. To send an alert: Check the **Send a network message to** check box, and enter the username or group name in the field.
13. To start a performance log: Check the **Start performance data log** check box, and choose the appropriate log type.
14. To run an external program: Check the **Run this program** check box, and enter the path and name of the program.
15. Click the **Schedule** tab. To assign the external program command line switches: Click **Command Line Arguments**, choose the desired switches, and click **OK**.
16. To automatically start the alert: Choose the **At** radio button and enter a date and time.
17. To never stop the alert: Choose the **Manually** option.
18. To stop the alert after a set number of seconds, minutes, hours, or days: Choose the **After** radio button and enter the number of units the system is to wait before stopping the counter log.
19. To stop the alert on a specific date and time: Choose the **At** option and enter the desired date and time.
20. Click **OK**.
21. Close the Performance console.

Project 8-5

1. Select **Start|Programs|Administrative Tools|Event Viewer**.
2. In the left pane, highlight the log that you would like to view.
3. In the right pane, double-click the event that you would like to view.
4. You can navigate to the previous and following events by clicking on the up and down arrow buttons respectively.
5. To finish, click **OK**.
6. Close the Event Viewer.

Project 8-6

1. Select **Start|Programs|Administrative Tools|Event Viewer**.
2. Right-click **Event Viewer (Local)** and choose the **Connect to another computer** option.
3. Enter the name of the remote computer, or click **Browse** to navigate to it.
4. Select the computer name. Click **OK**.
5. Close the Event Viewer.

Chapter 8 Case Projects

Case Project 8-1

One of your systems has started to perform poorly. When you check the Windows Task Manager you realize that the system is running with the CPU at 84% utilization. You also notice that the hard disks are "thrashing" (or being accessed repeatedly). You suspect that there is not enough physical memory (RAM) in the system. What would you do to confirm your theory?

Case Project 8-2

One of your systems paged you on Saturday night (using an alert), informing you that it had run out of disk space. The lack of disk space had caused this mission-critical system to "blue screen." You immediately drove to the office, installed an extra hard drive, and rebooted the system. The system, however, had been offline for several hours, making it inaccessible to your organization's clients worldwide. Monday morning you were asked to be present at an emergency meeting. In the meeting it was decided that the failure that occurred on the weekend could not be repeated, and that a solution must be found. It is your job to find a way to detect when a system is starting to get overloaded and running out of resources. What is your best course of action?

Chapter 9 Key Terms

authoritative restore — A process of restoring a Windows 2000 DC, in which the restored data is given precedence over the current Active Directory data on the network and is then replicated to all the other DCs. This method is normally used when objects in Active Directory have been deleted and need to be restored.

checkpoint file — A file that informs Active Directory which portion of the transaction log has been committed to the database and which has not.

Directory System Agent (DSA) — An agent that makes the data within Active Directory available to an application.

Extensible Storage Engine (ESE) — The underlying engine that physically stores the Active Directory data.

fully committed transaction — Any transaction that has been written to the database.

garbage collection — A process that runs every 12 hours on DCs and cleans up the transaction logs, getting rid of entries that are no longer of use.

non-authoritative restore — A process of restoring a Windows 2000 DC, in which the restored data is then overwritten by Active Directory replication.

online backup — The process of backing up the system without shutting down any of the services. The operating system and applications remain running during the backup process.

patch files — Used during an online backup to store any transactions that need to be written to the database (after the database has been backed up).

rolling back — The process of undoing changes that have not been fully written to the database.

system state data — Information about the system that is required for recovering the system during a failure. This information includes the Active Directory data, the system Registry, DNS, Certificate Server, and File Replication Service settings.

tombstone — A marker for marking deleted objects in Active Directory as deleted. This gives Active Directory time to replicate this change throughout the network.

tombstone lifetime — The amount of time a tombstone remains active in Active Directory. The default is 60 days.

transaction — A change being made to the database.

transaction log — A disk-based file that stores a list of all the transactions that have been applied to the Active Directory database. All transactions are recorded here before being written to the database.

Chapter 9 Review Questions

1. Active Directory uses two backup files when disk space on the system runs out. What are the names of these files?

   a. RES1.LOG

   b. RES2.LOG

   c. RES1.BAK
   d. RES2.BAK

2. Where are transactions written before they are committed to the Active Directory database?
   a. EDB.RES
   b. EDB.LOG
   c. EDB.CHK
   d. EDB.CMT

3. What is some of the critical system data that is stored in the system state data? (Choose all that apply.)
   a. The Registry
   b. Boot files
   c. DNS data
   d. All of the above

4. What is the default value of the tombstone lifetime in Windows 2000?
   a. 15 days
   b. 30 days
   c. 60 days
   d. 90 days

5. What kind of a restore is performed when you want the restored data to take precedence over the existing data?
   a. Offline
   b. Full
   c. Non-authoritative
   d. Authoritative

6. What kind of a restore is performed when you want the restored data to be replaced by the existing Active Directory data, using Active Directory replication?
   a. Offline
   b. Non-authoritative
   c. Full
   d. Authoritative

7. What is the default size of the Active Directory log files?
   a. 1 MB
   b. 5 MB
   c. 10 MB
   d. 20 MB

8. How often does the log cleanup occur on DCs?
    a. Every hour
    b. Every 3 hours
    c. Every 6 hours
    d. Every 12 hours
9. Which logging method creates a new log file when the old one is filled up?
    a. Circular logging
    b. Continuous logging
    c. Infinite logging
    d. None of the above
10. Which files should be placed on their own hard disks?
    a. NTDS.DIT
    b. Windows 2000 files
    c. Boot files
    d. Registry files
11. When an object is deleted in Active Directory, a marker is put in its place. What is that marker called?
    a. Deletion marker
    b. Tombstone
    c. Deletion flag
    d. Dead Object marker
12. When an object is deleted in Active Directory, a marker is put in its place to ensure:
    a. That fragmentation does not occur.
    b. That the object can be undeleted.
    c. That fragmentation does occur.
    d. That the fact that the object has been deleted is replicated to the other DCs.
13. Each DC cleans up its old data (such as committed log files) using which process?
    a. DC cleanup
    b. Garbage collection
    c. Garbage cleanup
    d. Log File cleanup
14. Which logging method overwrites log files when they fill up?
    a. Circular logging
    b. Continuous logging

c. Infinite logging

d. None of the above

15. What are the three layers of the Active Directory model?

a. Directory System Agent

b. Directory Storage Agent

c. Flexible Storage Engine

d. Extensible Storage Engine

e. The database layer

16. Which layer of the Active Directory model physically stores the AD data?

a. Directory System Agent

b. Flexible Storage Engine

c. Extensible Storage Engine

d. Directory Storage Agent

e. The database layer

17. Which layer of the Active Directory model processes the data hierarchically?

a. Directory System Agent

b. Flexible Storage Engine

c. Extensible Storage Engine

d. Directory Storage Agent

e. The database layer

18. Which layer of the Active Directory model controls security in the Directory?

a. Directory System Agent

b. Flexible Storage Engine

c. Extensible Storage Engine

d. Directory Storage Agent

e. The database layer

19. Which file contains pointers to the transactions that have not yet been committed to the database?

a. EDB.LOG

b. EDB.CHK

c. EDB.PAT

d. EDB.PNT

20. Which file is used during the backup process to store the transactions that have not been committed yet, although the database has already been backed up?

    a. EDB.LOG

    b. EDB.CHK

    c. EDB.PAT

    d. EDB.PNT

Chapter 9 Hands-on Projects

Project 9-1

1. Select **Start**|**Programs**|**Accessories**|**System Tools**|**Backup**.
2. Click **Backup Wizard**.
3. Click **Next**.
4. Choose one of the three options: Backup everything on my computer, Backup selected files, drives, or network data, or Only back up the System State data.
5. Click **Next**.
6. If you chose Back up selected files, drives, or network data in Step 4, choose the information that is to be backed up and click **Next**.
7. Select the Backup media type and the corresponding Backup media or file name, and click **Next**.
8. For Advanced options, click **Advanced** to select the Backup Type, to verify the backup, to use hardware compression, to append or replace existing data, to enter a label for the backup set and media, and to indicate whether to schedule the backup.
9. Click **Finish** to start the backup.
10. After the backup is complete, click **Close**.
11. Close the Backup utility.

Project 9-2

1. Select **Start**|**Programs**|**Accessories**|**System Tools**|**Backup**.
2. Click **Restore Wizard**.
3. Click **Next**.
4. Select the backup set to restore, and click **Next**.
5. For advanced features, click **Advanced** to select the restoration location and whether to replace files.
6. Click **Finish** to start the restore.
7. Click **Close**.
8. Close the Backup utility.

Project 9-3

1. Select **Start|Run**.
2. Type in **Regedt32** and click **OK**.
3. In the HKEY_LOCAL_MACHINE hive, navigate to System\CurrentControlSet\Services\NTDS\Parameters.
4. Add a new Value (from the Edit menu) with the name of **CircularLogging**.
5. Click **OK**.
6. Enter a string of **1**.
7. Click **OK**.
8. Close the Registry Editor.

Project 9-4

1. Select **Start|Run**.
2. Type in **Regedt32** and click **OK**.
3. In the HKEY_LOCAL_MACHINE hive, navigate to System\CurrentControlSet\Services\NTDS\Parameters.
4. Add a new Value (from the Edit menu) with the name of **CircularLogging**.
5. Click **OK**.
6. Enter a string of **0**.
7. Click **OK**.
8. Close the Registry Editor.

Chapter 9 Case Projects

Case Project 9-1

A junior administrator is on a work practicum with your organization. He has limited experience with Windows 2000 and Active Directory. On an especially busy day, you leave him alone in his office to answer the help desk while you are putting out some network fires. When you get back to the office, you notice that he is especially quiet and has a strange green tinge to his skin. After you grill him for answers for several minutes, he finally admits that he screwed up. Apparently, a manager called him, requesting that he delete a group in Active Directory that is no longer being used. He insisted that the manager wait for your return, but to no avail. He finally buckled under the pressure and ended up deleting an entire OU from the Active Directory domain. You calm him down and explain that you can simply recover last night's backup and recover the data. The two of you go to the server room and happily recover the lost OU on a backup DC that is reserved for situations such as this. After the DC is recovered, you show him that the deleted OU is back. However, when you try to make a change to the OU, AD returns an error. You refresh the display and, to your horror, the OU has disappeared again. What needs to be done to recover the OU?

Case Project 9-2

One of the hard disks in your DCs failed, and a complete backup does not exist. You explain this to your manager, but he tells you that he read somewhere that the Active Directory database is transactional and that it should be able to do an up-to-the-minute recovery using the backup copy of the database from last night's backup. You notice that the failed disk contained both the Active Directory database files and the transaction log files. Can the system be recovered, and, if not, how can you configure it to avoid this type of failure in the future?

Chapter 10 Key Terms

administrative templates — Built-in templates for providing a source for Group Policy to generate the policy settings that you can configure.

asynchronous processing — This type of processing allows policies to be processed without waiting for the outcome of other policies.

Group Policy namespace — The namespace covered by a specified GPO.

Group Policy Objects (GPO) — A collection of Group Policy settings.

local Group Policy Objects — Local GPOs exist on each Windows 2000 system, and by default only the settings under the Security node of the Group Policy apply.

monolithic design — This type of design uses a few very large GPOs and is often implemented at the site or domain level. The GPOs apply to all users and computers on the network, regardless of OU membership.

non-local Group Policy Objects — Non-local GPOs are stored on the domain within Active Directory.

Remote Installation Services (RIS) — A new Windows 2000 service for installing Windows 2000 Professional systems over the network.

return on investment (ROI) — A measure of the amount of time it takes in saved administrative resources to pay back for a product (in this case, Windows 2000).

segmented design — This type of design is associated with decentralized administrative control, because that type of environment is more likely to have multiple administrators and delegated control over Group Policy.

synchronous processing — This type of processing waits until one action is complete before beginning another.

total cost of ownership (TCO) — A measure of the amount of money a particular product costs (in this case, Windows 2000) to install, operate, and support.

CHAPTER 10 REVIEW QUESTIONS

1. Which of the following is a characteristic of a monolithic GPO design?
   a. Many small GPOs
   b. Multiple individual GPOs
   c. Few large GPOs
   d. One single GPO
2. Which of the following is a characteristic of a segmented GPO design?
   a. Many small GPOs
   b. Multiple individual GPOs
   c. Few large GPOs
   d. One single GPO
3. Which type of GPO is stored on the individual systems?
   a. Server
   b. Client
   c. Local
   d. Non-local
4. Which type of GPO is stored on the domain?
   a. Server
   b. Client
   c. Local
   d. Non-local
5. Which of the following tasks cannot be delegated?
   a. Managing GPOs
   b. Filtering GPOs
   c. Managing GPO links
   d. Editing GPOs
6. In which order are Group Policy settings applied during the logon process?
   a. Local, site, OU, domain
   b. Local, site, domain, OU
   c. Domain, site, OU, local
   d. Domain, site, local, OU
7. Which utility is used to delegate GPO editing?
   a. Group Policy snap-in
   b. GPO Editing snap-in

c. Active Directory Users and Computer

d. Active Directory Domains and Trusts

8. Which utility is used to delegate GPO creation?

a. Group Policy snap-in

b. GPO Editing snap-in

c. Active Directory Users and Computer

d. Active Directory Domains and Trusts

9. Which utility should be used to associate security settings with an entire site in your organization?

a. Active Directory Users and Computers

b. Group Policy snap-in

c. Active Directory Sites and Services

d. Group Policy Association snap-in

10. When you refresh a Group Policy, Folder Redirection is excluded. True or False?

a. True

b. False

11. A No Override setting is set only on which of the following?

a. Site

b. Domain

c. OU

d. Link

12. A Group Policy setting has three different states. Which of the following is not one of the states?

a. Enabled

b. Disabled

c. Configured

d. Not configured

13. You can use the EditSec tool to refresh Group Policy immediately. True or False?

a. True

b. False

14. When Group Policy detects a slow link, which of the following does not apply?

a. Folder Redirection is turned on.

b. Software Installation is turned off.

c. Internet Explorer maintenance is turned off.

d. Security Settings are always processed, regardless of link speed.

15. What is the default setting for a Group Policy setting?
    a. Enabled
    b. Disabled
    c. Configured
    d. Not configured
16. The process of associating a GPO with an object is known as ______________.
    a. Joining
    b. Linking
    c. Matching
    d. Grouping
17. What should be used to ensure that a Group Policy setting is applied throughout the domain?
    a. No Override
    b. Block Policy Inheritance
    c. Allow Policy Inheritance
    d. Allow Override
18. Which of the following is a definition of synchronous processing?
    a. All processing takes place at once.
    b. All processes are processed one at a time.
    c. Only one process can be executed for every instance of the object.
    d. None of the above
19. Which of the following is a definition of asynchronous processing?
    a. All processing takes place at once.
    b. All processes are processed one at a time.
    c. Only one process can be executed for every instance of the object.
    d. None of the above
20. Administrative templates created with the Windows NT 4.0 System Policy Editor can be read and changed with the Windows 2000 System Policy Editor. True or False?
    a. True
    b. False

CHAPTER 10 HANDS-ON PROJECTS

Project 10-1

1. Select **Start|Programs|Administrative Tools|Active Directory Users and Computers**.
2. Right-click on the domain and choose the **New|Organizational Unit** option.
3. Enter a name for the new OU, then click **OK**.
4. Right-click on the OU and choose the **Properties** option.
5. Select the **Group Policy** tab.
6. Click **New**.
7. Enter a name for the new GPO.
8. Click **Close**.
9. Close the Active Directory Users and Computers console.

Project 10-2

1. Select **Start|Programs|Administrative Tools|Active Directory Users and Computers**.
2. Right-click on the OU and choose the **Properties** option.
3. Select the **Group Policy** tab.
4. Highlight the GPO created in Hands-on Project 10-1, and click **Properties**.
5. Select the **Security** tab.
6. Click **Add** to add users and computers to which this GPO should apply, then click **OK**.
7. Specify the desired permissions.
8. Click **OK**, then click **OK** again.
9. Close the Active Directory Users and Computers console.

CHAPTER 10 CASE PROJECTS

Case Project 10-1

You are the lead administrator for a medium-sized company. Your organization has purchased a competitor. The competitor's network will be joined with yours, but they do not have any full-time administrators on-site. Instead, they contract an IT firm to do the network support for them. While you do not want to give the IT firm full access to your Active Directory tree, you need to grant them some rights. What would be the best course of action to accomplish this?

Case Project 10-2

You inherit a Windows 2000 network, and you realize that the password policy has not been modified from the default settings. From your experience, you know that the default security is not secure enough for most installations. What do you need to do to secure the password settings?

Chapter 11 Key Terms

computer template — An administrative template that controls the configuration of a computer.

File Replication service (FRS) — The replacement to the Windows NT Directory Replication service. This service replicates the entire SYSVOL directory tree across all Windows 2000 domain controllers.

folder redirection — A new feature of Windows 2000 that is essentially the process by which the operating system changes the location of certain Windows 2000 folders from the local hard drive to a specified network share. The folders that can be redirected include: Application Data, Desktop, My Documents, My Pictures, and Start Menu.

logoff script — A script that executes when the user logs off the system.

logon script — A script that executes when the user logs on to the system. This script runs under the account with which the user is associated.

shutdown script — A script that runs when the computer is being shut down. It is executed under the Local System account.

startup script — A computer script that is executed under the Local System account during the computer startup process, before the user logon screen is displayed.

user template — An administrative template that controls the configuration of a user.

Windows Scripting Host (WSH) — A scripting host that allows for the execution of VBScript (.vbs) and JavaScript (.js) natively on 32-bit Windows platforms.

Chapter 11 Review Questions

1. Windows 2000 folder redirection allows an administrator to redirect any folder on the system to a network share. True or False?

   a. True

   b. False

2. Which of the following folders cannot be redirected using the Windows 2000 folder redirection service?

   a. My Documents

   b. Documents and Settings

   c. Start Menu

   d. Desktop

3. What is the DOS-based Windows Scripting Host file?
    a. CScript.exe
    b. WScript.exe
    c. Jscript.exe
    d. VBScript.exe
4. What is the Windows-based Windows Scripting Host file?
    a. CScript.exe
    b. WScript.exe
    c. Jscript.exe
    d. VBScript.exe
5. Which script is applied to the computer when it first starts up?
    a. Boot
    b. Login
    c. Startup
    d. Begin
6. Which script is applied to the computer when it is turned off?
    a. Login
    b. Startup
    c. Shutdown
    d. Down
7. In which order do the Windows 2000 scripts execute?
    a. Logon, logoff, startup, shutdown
    b. Logon, startup, shutdown, logoff
    c. Startup, logon, logoff, shutdown
    d. Logon, startup, shutdown, shutdown
8. Which file extension does WSH 1 use?
    a. .ws
    b. .wsh
    c. .wsf
    d. .ws1
9. Which file extension does WSH 2 use?
    a. .ws
    b. .wsh
    c. .wsf
    d. .ws2

10. With version 2 of WSH, the .vbs and .js files are replaced by the .WSF file. True or False?

    a. True

    b. False

11. Which Registry hive is modified by the computer policies?

    a. HKEY_CURRENT_USER

    b. HKEY_LOCAL_MACHINE

    c. HKEY_CLASSES_ROOT

    d. HKEY_USERS

12. Microsoft has included a variable that directly relates to the name of the user who is currently logged on to the system. This variable can be used with FRS. What is this variable?

    a. username

    b. user

    c. %username%

    d. %user%

13. Custom administrative templates have which of the following extensions associated with them?

    a. .adm

    b. .tmp

    c. .txt

    d. .inf

14. Which of the following two languages are supported in WSH?

    a. JavaScript

    b. Java

    c. VBScript

    d. REXX

15. Which file in WSH version 1 is used simply for formatting the output of a script?

    a. WSH

    b. WSF

    c. WS

    d. WS1

16. Which of the following are entries that are used when creating administrative templates?

    a. POLICY

    b. SECTION

c. CLASS

d. CATEGORY

17. Double-clicking on a .VBS file will execute it. True or False?

a. True

b. False

18. Which of the following administrative templates exists only under User Configuration?

a. Network

b. System

c. Control Panel

d. Windows Components

19. Although only JavaScript and VBScript are supported natively by WSH version 2, it is possible to install other languages, such as Perl. True or False?

a. True

b. False

20. GPO has a "miscellaneous" category for policies. What is the name of that category?

a. Control Panel

b. System

c. Network

d. Windows Components

Chapter 11 Hands-on Projects

Project 11-1

1. Select **Start|Programs|Administrative Tools|Active Directory Users and Computer**.
2. Right-click on the domain, and choose the **Properties** option.
3. Select the **Group Policy** tab.
4. Click **New** to create a new Group Policy, then name the new Group Policy.
5. Highlight the Group Policy and click **Edit**.

Project 11-2

1. In the Group Policy utility, navigate to the Desktop object (**User Configuration| Administrative Templates|Desktop**).

2. Double-click the **Disable adding**, **dragging**, **dropping, and closing the Taskbar's toolbars** option.
3. Choose the **Enabled** option and click **OK**.
4. Double-click on the **Don't save settings at exit** option.
5. Choose the **Enabled** option and click **OK**.

Project 11-3

1. In the Group Policy utility, navigate to the Active Desktop object (**User Configuration|Administrative Templates|Desktop|Active Desktop**).
2. Double-click the **Active Desktop Wallpaper** option.
3. Choose the **Enabled** option.
4. Enter a path and a name for the wallpaper file.
5. If necessary, choose the wallpaper style.
6. Click **OK**.

Project 11-4

1. In the Group Policy utility, navigate to the System object (**Computer Configuration|Administrative Templates|System**.
2. Double-click the **Disable Autoplay** option.
3. Choose the **Enabled** option.
4. Choose to disable Autorun on either all drives or on CD-ROM drives, from the drop-down menu.
5. Click **OK**.

Project 11-5

1. In the Group Policy utility, navigate to the Control Panel object (**User Configuration|Administrative Templates|Control Panel**.
2. Double-click the **Disable Control Panel** option.
3. Choose the **Enabled** option and click **OK**.

Project 11-6

1. In the Group Policy utility, navigate to the Logon/Logoff object (**User Configuration|Administrative Templates|System|Logon/Logoff**.
2. Double-click the **Disable Logoff** option.
3. Choose the **Enabled** option and click **OK**.
4. Close the Group Policy utility, click **OK** in the domain Properties page, and then close the Active Directory Users and Computers console.

Chapter 11 Case Projects

Case Project 11-1

Your organization donates one of its labs on the weekends to a local school. The school brings in a group of students to learn all about computers. The problem is that several of the students have "learned too much." You find that when you return to the lab on Monday morning, you have to completely rebuild the lab. How can you configure the lab network (all systems are running Windows 2000) so that the students cannot modify the desktop?

Case Project 11-2

In looking for a way to back up user data, your organization has decided that purchasing a backup agent program for each workstation is simply too costly. You are therefore given a project to find another solution, using the fewest resources possible. You need to back up data such as the user's My Documents, Start Menu, and Application Data files. How would you accomplish this with Windows 2000?

Chapter 12 Key Terms

change and configuration management — A collection of ideas and strategies for reducing TCO and increasing ROI.

distribution phase — The process of distributing applications to your users and systems from central distribution points.

distribution point — A network share or shares from which users can install software.

hard costs — The actual cost of the hardware and software for systems.

installation phase — In this phase, the software is rolled out across the organization to all users and computers that are configured to receive it.

IntelliMirror — A Windows 2000 feature that seeks to increase the availability of Windows 2000-based computers while decreasing total cost of ownership.

Internet Information Server (IIS) — Microsoft's built-in Web server.

just-in-time (JIT) — The technology that allows applications to be available to users whenever they log on to a system or launch an application, no matter where or when they log in.

offline folders — A Windows 2000 feature that allows users to ensure that important documents that are usually stored on the server are made available to them if the server is offline, the network is unavailable, or the system is no longer connected to the network.

Outlook Web Access (OWA) — A component of Exchange Server that allows users to access their e-mail accounts via the Internet.

patching applications — The process of upgrading or fixing applications that have already been installed, without the need to reinstall them. This is similar to applying a hot fix or a service pack in Windows 2000.

pilot phase — In the pilot phase, a pilot program is performed. A pilot program is a trial run deployed first in a lab environment and then to a subset of users, for the express purpose of troubleshooting and debugging any application issues prior to the full deployment.

preparation phase — The preparation phase of software management consists of the initial information collection process, including the analysis of the organization's structure to determine its software requirements.

soft costs — The cost of IT infrastructure. These costs include the cost for the support team and for the employees using the systems.

targeting phase — The targeting phase of software management consists of the creation of Group Policy to create and/or modify Group Policy Objects, in order to target the software to specific users and groups.

transforms — Transforms, which are the MST files that Windows Installer uses, are used to customize the installation of applications, changing them from their default behavior.

universal naming convention (UNC) — An industry standard naming convention for accessing network resources. UNC takes the form of \\server\share. For example, to access the users folder on the server named mainserver, the UNC would be \\mainserver\users.

ZAP file — A ZAP file contains settings relevant to controlling a program's appearance and behavior. It is similar to the old INI files and is used in non-Windows Installer packages.

Zero Administration Windows (ZAW) — The predecessor to IntelliMirror, Microsoft's original initiative to create a managed desktop environment under Windows.

Chapter 12 Review Questions

1. Which phase of software management involves testing the software installation in a controlled environment?
   a. Preparation
   b. Distribution
   c. Targeting
   d. Pilot
   e. Installation
2. Which phase of software management involves analysis of the network to determine the software requirements?
   a. Preparation
   b. Distribution
   c. Targeting
   d. Pilot
   e. Installation

3. Which phase of software management involves the creation of GPOs to deploy the software to the appropriate users?
    a. Preparation
    b. Distribution
    c. Targeting
    d. Pilot
    e. Installation
4. Which phase of software management involves the actual installation of the software to the targeted group of users or computers?
    a. Preparation
    b. Distribution
    c. Targeting
    d. Pilot
    e. Installation
5. Which phase of software management involves the sharing of the installation packages on network servers?
    a. Preparation
    b. Distribution
    c. Targeting
    d. Pilot
    e. Installation
6. Microsoft has produced and sells a product whose features far exceed what can be done with GPOs and IntelliMirror. What is that product?
    a. Microsoft Exchange Server
    b. Microsoft System Management Server
    c. Microsoft SQL Server
    d. Microsoft ISA Server
7. A non-Windows Installer package has which extension when it is deployed with Software Installation?
    a. .ini
    b. .zip
    c. .zap
    d. .msf

8. Which file extension does a Microsoft Windows Installer file use?
   a. .zap
   b. .msf
   c. .msi
   d. .inf
9. What is the term used to describe the network share in which Windows Installer packages are placed before being deployed out to users and computers?
   a. mount point
   b. share point
   c. install point
   d. distribution point
10. A soft cost is described as any cost associated with software purchases and upgrades. True or False?
    a. True
    b. False
11. When you are patching an application, which of the following modifications can be performed by Windows Installer?
    a. Hardware settings
    b. Services
    c. Files
    d. Registry entries
12. Which phase of the software deployment strategy is usually not completed?
    a. Preparation
    b. Distribution
    c. Targeting
    d. Pilot
    e. Installation
13. Which of the following is a requirement of Software Installation on a Windows 2000 system?
    a. Active Directory
    b. DVD drive
    c. 512 MB of RAM
    d. 2 GB of disk space

14. Which extension does a transform file use?
    a. .mst
    b. .msi
    c. .msf
    d. .mso
15. An assigned package is a package that is automatically installed on users' systems. They do not get the option not to install the package. True or False?
    a. True
    b. False
16. A published package is a package that is automatically installed on users' systems. They do not get the option not to install the package. True or False?
    a. True
    b. False
17. Which two components of WinINSTALL are included with Windows 2000?
    a. Watcher
    b. Software Console
    c. INSTALLConsole
    d. Discover
18. What is the correct order of the software deployment phases?
    a. Installation, preparation, targeting, distribution, pilot
    b. Preparation, installation, pilot, distribution, targeting
    c. Installation, pilot, targeting, distribution, preparation
    d. Preparation, distribution, targeting, pilot, installation
19. Which application is used to patch an existing .MSI package?
    a. VERITAS Discover
    b. VERITAS Repair Console
    c. VERITAS Software Console
    d. VERITAS Patch
20. What are .MSI modifications known as?
    a. Patches
    b. Modifications
    c. Changes
    d. Transforms

CHAPTER 12 HANDS-ON PROJECTS

Project 12-1

1. Insert the Windows 2000 Server CD into the CD-ROM drive. If Auto run starts, exit the program.
2. Navigate to the **valuadd\3rdparty\mgmt\winstle** folder.
3. Double-click on the **SWIADMLE.MSI** file.

Project 12-2

1. Select **Start**|**Programs**|**VERITAS Software**|**VERITAS Discover**.
2. Click **Next**.
3. Enter a name for the application for which you are building the installation.
4. Choose a path on the system for the .msi file.
5. Click **Next**.
6. Choose a drive where Discover can store temporary files.
7. Click **Next**.
8. In the left pane, choose the drive or drives to be scanned, and click **Add**.
9. Click **Next**.
10. In the left pane, choose any files or folders to be excluded from the scan, and click **Add**.
11. Click **Next**.
12. Once the scan is completed, click **OK**, then navigate to and select the installation file.
13. Select **Start**|**Programs**|**VERITAS Software**|**VERITAS Discover**.
14. Ensure that the **Perform the "After" snapshot now** radio button is selected.
15. Click **Next**.
16. Click **OK**, then click **OK** again.

Project 12-3

1. Select **Start**|**Programs**|**Administrative Tools**|**Active Directory Users and Computers**.
2. Choose a test OU.
3. Right-click on the OU and choose the **Properties** option.
4. Choose the **Group Policy** tab.
5. Choose a GPO and click **Edit**.
6. Navigate to the Software installation container under **User Configuration**|**Software Settings**.

7. Right-click **Software installation** and choose **New|Package**.
8. Navigate to the created .msi file and click **Open**.
9. Choose the **Published** option and click **OK**.

Project 12-4

1. Select **Start|Programs|Administrative Tools|Active Directory Users and Computers**.
2. Choose a test OU.
3. Right-click on **OU** and choose the **Properties** option.
4. Choose the **Group Policy** tab.
5. Choose a GPO and click **Edit**.
6. Navigate to the Software Installation container under **User Configuration|Software Settings**.
7. Right-click **Software installation** and choose **New|Package**.
8. Navigate to the created .msi file and click **Open**.
9. Choose the **Assigned** option and click **OK**.

Chapter 12 Case Projects

Case Project 12-1

At a weekly departmental meeting, it is made clear that a large portion of a couple of IT support staff members' time is spent simply fixing broken applications. Many of your users are only computer literate enough to be dangerous, and they tend to delete files that they feel are not needed, thereby breaking applications on their systems. Your organization has looked at products such as Microsoft's SMS, but the cost of the product and the subsequent infrastructure and support costs make it impossible for you to implement. You therefore need to find an inexpensive solution for automatically checking applications and reinstalling missing files, or the entire application, should the need arise. What Windows 2000 technology can you use to accomplish this?

Case Project 12-2

You did such a fine job solving the "file-deleting user" problem that your manager decided to give you another project. This project entails automating the installation of applications on users' systems. The catch is that you do not want to install all applications on all systems by default, only the ones that the users require. How would you accomplish this?

Chapter 13 Key Terms

Boot Information Negotiation Layer (BINL) — A server-side service that provides a default set of screens to the user.

Client Installation Wizard — The client-side component of RIS. This component is downloaded to the client and communicates with RIS.

Pre-Boot Execution Environment (PXE) — An industry standard for enabling a compliant client PC to gain basic TCP/IP network connectivity automatically.

prestaging — A process used to create computer accounts in advance of installation and to ensure that each computer name is unique.

Remote Installation Services (RIS) — A Windows 2000 service for quickly installing Windows 2000 Professional on systems using the PXE protocol.

RIPrep — A utility used to create Windows 2000 Professional images with customized settings and locally installed desktop applications.

RISetup — A utility used to configure RIS and create Windows 2000 Professional images.

Single Instance Store (SIS) — A service that reduces disk space requirements for RIS images by combining duplicate files.

Trivial File Transfer Protocol Daemon (TFTPD) — A service used by RIS to download the initial client files necessary to begin the Windows 2000 Professional installation.

Chapter 13 Review Questions

1. Which application should you use when creating a network-based installation of Windows 2000?
   a. Winnt32.exe
   b. RIPrep.exe
   c. Winnt.exe
   d. RISetup.exe

2. In which application can an RIS boot disk be created?
   a. RIPrep.exe
   b. RISDisk.exe
   c. RISetup.exe
   d. RBFG.exe

3. Which of the following files can be found on an RIS boot disk?
   a. Ntldr
   b. Boot.ini
   c. RISDISK
   d. Ntdetect.com

4. When you install RIS on a Windows 2000 system, which of the following file system or file systems is required?
   a. FAT16
   b. FAT32
   c. NTFS
   d. CDFS
5. When you want to authorize an RIS server for increased security on the network, which utility do you use?
   a. Active Directory Users and Computers
   b. Active Directory Domains and Trusts
   c. The DNS snap-in
   d. The DHCP snap-in
6. RIS includes a service that saves the disk space required by the images by eliminating duplicate files. What is the name of the service?
   a. SRS
   b. SIS
   c. BINL
   d. TFTPD
7. Which of the following is NOT a requirement for installing RIS?
   a. Active Directory
   b. Domain Name System
   c. Dynamic Host Configuration Protocol Service
   d. Windows Internet Naming Service
8. Which of the following standards must a client computer meet in order to use RIS? Choose all that apply.
   a. NetPC
   b. MPC
   c. PC98
   d. PC97
9. If a system does not meet the required standards and the network card is not PXE-compliant, it might still be possible to use RIS with it. True or False?
   a. True
   b. False

10. RIS cannot be installed if the server is running a Distributed File System (DFS) volume. True or False?
    a. True
    b. False
11. What is the minimum processor required for running RIS?
    a. Pentium 166
    b. Pentium 200
    c. Pentium Celeron 400
    d. Pentium III 650
12. What is the term used when the administrator configures the computer accounts in Active Directory before the systems are installed?
    a. Preconfiguration
    b. Precreation
    c. Premodification
    d. Prestaging
13. For which operating systems can RIPrep be used to create images? Choose all that apply?
    a. Windows NT Workstation
    b. Windows NT Server
    c. Windows 2000 Professional
    d. Windows 2000 Server
14. When an image creation fails, where does RIPrep log its status and error messages?
    a. RIPrep.log
    b. RIPrep.err
    c. RIPrep.aud
    d. RIPrep.txt
15. What does RIS use the Trivial File Transfer Protocol Daemon for?
    a. Uploading the entire Windows 2000 image to the client
    b. Uploading the files necessary to begin the Windows 2000 Professional installation to the client
    c. Uploading the files needed for the Client Installation Wizard
    d. Authenticating with Active Directory
16. Which of the following does the Boot Information Negotiation Layer (BINL) *not* do?
    a. Listen to DHCP/PXE requests
    b. Verify logon credentials with Active Directory

c. Redirect clients to the appropriate files needed for the installation during the Client Installation Wizard

d. Download all files necessary to begin the Windows 2000 Professional installation

17. RIS can be installed if the server is running an Encrypted File System (EFS) volume. True or False?

    a. True

    b. False

18. What is the name of the bootstrap program that displays the message for the user to press F12 for Network Service?

    a. Bootstrap.exe

    b. Netboot.exe

    c. Startrom.exe

    d. Netdetect.exe

19. Which file contains the installation information about the image's source computer, such as the installation directory and the HAL type?

    a. RIPrep.dat

    b. Bootcode.dat

    c. Lmirror.dat

    d. HAL.dat

20. Which file contains the boot sector information for the client computer?

    a. RIPrep.dat

    b. Bootcode.dat

    c. Lmirror.dat

    d. HAL.dat

Chapter 13 Hands-on Projects

Project 13-1

1. Select **Start|Settings|Control Panel**.
2. Double-click **Add/Remove Programs**.
3. Click the **Add/Remove Windows Components** button from the left pane.
4. Select the **Remote Installation Services** checkbox.
5. Click **Next**. If necessary, insert the Windows 2000 Server CD-ROM and then click **OK**.
6. Click **Finish**.

7. Reboot the server if necessary. Open the **Add/Remove Programs** applet again if necessary.
8. In the Add/Remove Programs applet, select the **Add/Remove Windows Components** button from the left pane, select the **Configure Remote Installation Services** option, and click **Configure**.
9. Click **Next**.
10. Enter the folder path where you want the root of the Remote Installation Services operating system images to reside, and click **Next**.
11. If you want the RIS to start immediately, select the **Respond to client computers requesting service** check box, and click **Next**.
12. Enter the path to the Windows 2000 Professional installation files, and click **Next**.
13. Enter a name for the folder that will be created to store the operating system image, and click **Next**.
14. Enter a friendly description for this operating system image, and click **Next**.
15. Click **Finish**.
16. Click **Done** when the Remote Installation Services Setup Wizard tasks are completed, then close the Add/Remove Programs applet and the Control Panel.

Project 13-2

1. Select **Start**|**Programs**|**Administrative Tools**|**Active Directory Users and Computers**.
2. Navigate to the server where you would like to enable RIS, right-click on it, and choose the **Properties** option.
3. Click the **Remote Install** tab.
4. Select the **Respond to client computers requesting service** check box, if necessary, and click **OK**.
5. Close the Active Directory Users and Computers console.

Project 13-3

1. Select **Start**|**Programs**|**Administrative Tools**|**Active Directory Users and Computers**.
2. Navigate to the server running RIS, right-click on it, and choose the **Properties** option.
3. Click the **Remote Install** tab.
4. Click the **Advanced Settings** button.
5. Select the **Images** tab, then click the **Add** button.

6. Indicate whether a new answer file is being used for an existing image, or create a new image from the Windows 2000 Professional installation files, and select the **Add a new installation image** option.
7. Click **Next**.
8. Follow the steps in the Remote Installation Services Setup Wizard.
9. Click **OK** in the Remote Installation Services Properties window, then click **OK** in the server Properties page.
10. Close the Active Directory Users and Computers console.

Project 13-4

1. Install Windows 2000 Professional on a reference system using RIS.
2. Install any applications that are to be duplicated in the image.
3. Configure the system as required.
4. Shut down all services and applications.
5. Run the RIPrep.exe application from the RemoteInstall\Admin\i386 share on the RIS system. Your share name might be different.
6. Click **Next**.
7. Enter the name of the RIS server that you would like to host the image, and click **Next**.
8. Enter the folder name where the image will be stored, and click **Next**.
9. Enter a friendly description for the image, and click **Next**.
10. Click **Next**.
11. To copy the image to the RIS server, click **Next** in the Programs or Services are Running screen, click **Next** in the Review Settings screen, and then click **Next** to start copying.

Project 13-5

1. Insert a blank, formatted 1.44 MB floppy disk, connect to the RIS server's \RemoteInstall\Admin\i386 share, and run the rbfg.exe file.
2. Click **Create Disk**. Click **No** when asked if you'd like to create another disk.
3. Click **Close** in the Windows 2000 Remote Book Disk Generator window.

Project 13-6

1. Shut down the system.
2. Insert the Remote Boot Disk and turn on the system.
3. Press the **F12** button to boot from the network.
4. Press **Enter** to begin the Client Installation Wizard.

5. Enter a username, a password, and the DNS name for the domain, and press **Enter**.
6. Choose the Automatic Setup, Custom Setup, Restart a Previous Setup Attempt, or Maintenance and Troubleshooting Tools option, and press **Enter**.
7. Select the image that you would like to use, and press **Enter**.
8. Press **Enter**.

Chapter 13 Case Projects

Case Project 13-1

Your organization has purchased a large number of new systems. You are looking for the best and quickest way of installing Windows 2000 Professional on these systems. Your organization has not tested any technologies such as Ghost and therefore will not purchase such technologies. You check the systems and confirm that they are PXE-compliant. What would be the best way to accomplish your goals?

Case Project 13-2

After you quickly installed Windows 2000 Professional on all the new systems, management decided to do the same to the older, non-Windows 2000 systems. You check them out and realize that they are not PXE-compliant. How would you go about installing Windows 2000 Professional on the systems, using RIS?

Chapter 14 Key Terms

convergence — A term used to describe a network in which all DCs are 100% up to date. That is to say, there are no more changes to be replicated.

high-watermark table — A table stored at the DC, which stores the name of each of the DC's replication partners, along with the last known USN value for that DC.

latency — A term describing the inherent delay in Active Directory replication.

originating update — An originating update is the first time a change is made to a property in Active Directory.

propagation dampening — A term used to describe the process used by Active Directory to ensure that changes don't endlessly loop around a Windows 2000 network.

Property Version Number (PVN) — A value that is appended to every property within Active Directory and traces the number of times a specific property has been changed.

replicated update — A replicated update is a change made to Active Directory that did not originate at that copy.

replication partners — A group of DCs that replicate Active Directory data among themselves.

Update Sequence Number (USN) — A 64-bit number that keeps track of changes as they are written to copies of Active Directory.

up-to-date vector table — A table that stores a list of every DC on the network, along with the USN of the last originating update made on that DC.

Chapter 14 Review Questions

1. When replication partners are automatically calculated, what is the maximum number of hops that can exist between them?
   a. 2
   b. 3
   c. 4
   d. 5
2. What is the term used to describe the delay associated with Active Directory replication?
   a. Latency
   b. Convergence
   c. Replication latency
   d. Replication delay
3. What is the term used to describe a network in which no more Active Directory changes need to be replicated?
   a. Latency
   b. Convergence
   c. Replication latency
   d. Replication delay
4. What is a group of DCs that replicate Active Directory data to each other called?
   a. Replication group
   b. Replication block
   c. Replication pair
   d. Replication partners
5. Which of the following are the two types of Windows 2000 replication updates?
   a. Originating update
   b. First update
   c. Replicated update
   d. Duplicated update

6. By what value does an Update Sequence Number (USN) increment?
   a. 1
   b. 2
   c. 3
   d. 4
7. Which table is used to store the USN value only for each DC with which a DC replicates?
   a. Up-to-date vector table
   b. USN table
   c. High-watermark table
   d. KCC table
8. Which table is used to store the USN value at the time of the last originating update for each DC within the domain?
   a. Up-to-date vector table
   b. USN table
   c. High-watermark table
   d. KCC table
9. Active Directory replication uses a pull technology, rather than push. True or False?
   a. True
   b. False
10. Active Directory replication that occurs between DCs in a site is known as ________________.
    a. Remote replication
    b. Intersite replication
    c. Intrasite replication
    d. Local replication
11. Active Directory replication that occurs between DCs in different sites is known as ________________.
    a. Remote replication
    b. Intersite replication
    c. Intrasite replication
    d. Local replication
12. What keeps track of how many times a record has been modified?
    a. USN
    b. VPN

c. PVN

d. KCC

13. When all Active Directory replication between sites is directed through a specific server, what is the name given to that server?

a. Gateway server

b. Bridge server

c. Controller server

d. Bridgehead server

14. What is the Windows 2000 Active Directory replication model called?

a. Multi-master

b. No-Master

c. Single-Master

d. None of the above

15. With multiple DCs replicating with multiple other DCs, it is possible for replication data to be replicated repeatedly. What did Microsoft include in Windows 2000 to solve this problem?

a. Propagation dampening

b. Propagation termination

c. Propagation resistance

d. Propagation control

16. What does the acronym USN stand for?

a. Universal Sequence Number

b. Unique Sequence Number

c. Update Sequence Number

d. Upgrade Sequence Number

17. The higher the cost of a site link, the more attractive it is to Active Directory replication. True or False?

a. True

b. False

18. When replicated between two different sites, data can be compressed. True or False?

a. True

b. False

19. When replication takes place within a site, replication can be scheduled. True or False?

a. True

b. False

20. There are two tables stored on each DC that assist in Active Directory replication. What are they called?
    a. Up-to-date vector table
    b. USN table
    c. High-watermark table
    d. KCC table

Chapter 15 Key Terms

archiving — The process of making a copy of an event log for review at a later date.

basic scenario — Any template designed to return the system to the default settings if any have been changed.

compat scenario — This template is a compatible template that makes the system compatible with previous versions of Windows.

hisec scenario — These templates are designed to secure systems for network communication.

local policy — A Group Policy set to a single, local machine.

secure scenario — This template is the recommended template for a system. It enforces all the suggested security features.

security template — A collection of prebuilt templates that alter auditing and security settings.

system policy — A Group Policy set to a group of systems over the network.

tattooing — A feature in which the value of a key is changed from one value to another, and the original value is not stored.

Chapter 15 Review Questions

1. Which security template should be used to ensure that these security settings will work with previous versions of Windows?
    a. Basic
    b. Compat
    c. Secure
    d. Hisec
2. Which security template should be used to provide the highest security to the system?
    a. Basic
    b. Compat
    c. Secure
    d. Hisec

3. Which security template should be used to return a system to its default security settings?
   a. Basic
   b. Compat
   c. Secure
   d. Hisec
4. Which security template should be used to secure a system with the recommended settings?
   a. Basic
   b. Compat
   c. Secure
   d. Hisec
5. Which extension is associated with the security templates?
   a. .cfg
   b. .sec
   c. .dat
   d. .inf
6. You specify which events to audit in the object's properties, but the Security event log remains blank. What might be the reason for this?
   a. Audit events are located in the audit logs, not the Security Logs.
   b. While the events to be audited are configured, auditing is not enabled on the system.
   c. The auditing service has incorrect credentials and cannot connect to the logging service.
   d. None of the above
7. Once the Security Templates are created, which tool would you use to apply them to servers on the network?
   a. Security Templates snap-in
   b. Security Configuration and Analysis snap-in
   c. Active Directory Users and Computers
   d. Security Policies snap-in
8. Once the security templates are created, which tool would you use to test how they will affect the servers on the network?
   a. Security Templates snap-in
   b. Security Configuration and Analysis snap-in

   c. Active Directory Users and Computers

   d. Security Policies snap-in

9. What is the correct syntax for forcing the Group Policy changes to propagate?

   a. Secedit /refresh machine_policy

   b. Secedit /propagate machine_policy

   c. Secedit /forcerefresh machine_policy

   d. Secedit /refreshpolicy machine_policy

10. Where are the predefined security templates stored?

    a. *Systemroot*\System32\Security

    b. *Systemroot*\Security\Templates

    c. *Systemroot*\System32\Templates

    d. *Systemroot*\Templates\Security

11. Which utility is used to create and modify the security templates?

    a. Security Templates snap-in

    b. Security Management snap-in

    c. Active Directory Users and Computers

    d. Security Policies snap-in

12. When policy changes are made in Group Policy, which of the following is not an option for speeding up the time it takes to propagate the changes through the network?

    a. Wait for the change to propagate.

    b. Reboot the system.

    c. Use Secedit to force the propagation.

    d. There is nothing that can be done.

13. When Windows 2000 is first installed, which events are audited automatically?

    a. No events are audited.

    b. Only successful audits.

    c. Only unsuccessful audits.

    d. All events are audited.

14. You should turn on all auditing events (both successes and failures) on your network to ensure that no unauthorized access is gone undetected. True or False?

    a. True

    b. False

15. It is a requirement in your organization to archive all log files for future reference. What is the best way of doing this without creating a few, very large log files?
    a. Save the .evt files and store them off the network (such as on a CD-ROM disk).
    b. Increase the audit log file size to 2 GB.
    c. Do nothing. Windows 2000 automatically archives the data.
    d. None of the above

Chapter 15 Hands-on Projects

Project 15-1

1. Select **Start**|**Programs**|**Administrative Tools**|**Domain Security Policy**.
2. Expand Security Settings, expand Local Policies, and then select **Audit Policy**. Double-click the audit policy that is to be enforced.
3. Indicate whether to audit successes, failures, or both, and click **OK**.
4. Close the Domain Security Policy console.

Project 15-2

1. Open the Active Directory Sites and Services console. Right-click on the object that you would like to audit, and choose the **Properties** option.
2. Select the **Security** tab.
3. Click **Advanced**.
4. Select the **Auditing** tab.
5. To add a user or group, click **Add**, select the user/group, click **OK**, select the access to audit, click **OK**, and then click **OK** in the Access Control Settings page.
6. To remove a user or group, highlight the user/group and click **Remove**.
7. Click **OK**.
8. Click **OK**.
9. Close the Active Directory Sites and Services console.

Project 15-3

1. Select **Start**|**Run**.
2. Type in **MMC** and click **OK**.
3. Select **Add/Remove Snap-in** from the Console menu.
4. Click **Add**.
5. Select **Security Templates** and click **Add**.

6. Select **Security Configuration and Analysis**, then click **Add**.
7. Click **Close**.
8. Click **OK**.
9. Select the **Save** option from the Console menu.
10. Enter a name for the MMC console, and click **Save**.

Project 15-4

1. Select the Security Templates snap-in configured in Hands-on Project 15-3.
2. Double-click on the default path folder.
3. Right-click on the security template that you would like to change, and choose the **Save As** option.
4. Enter a new name for the template, and click **Save**.
5. Double-click on the newly created template.
6. Modify the security settings.

Project 15-5

1. Select the Security Templates snap-in configured in Hands-on Project 15-3.
2. Right-click on the default path folder, and choose the **New Template** option.
3. Enter a name and description for the new security template, and click **OK**.
4. Double-click on the newly created security template.
5. Modify the security settings.

Project 15-6

1. Select the Security Templates snap-in configured in Hands-on Project 15-3.
2. Right-click **Security Configuration and Analysis**, and choose the **Open database** option.
3. Enter a database name to open, and click **Open**.
4. Right-click on **Security Configuration and Analysis**, then select **Import Template**. Select the template to import and click **Open**.
5. Right-click **Security Configuration and Analysis**, and choose **Configure Computer Now**.
6. Enter the error Error log file path and click **OK**.
7. Close the MMC Console.

Chapter 15 Case Projects

Case Project 15-1

You suspect that a hacker is attempting to access your network by using a password attack on your domain. You need to configure auditing so that it captures any relevant information about the hacker. Your organization will be taking legal action against the hacker and would like as much information as possible. How would you configure your system to capture this information?

Case Project 15-2

After taking a class on Windows 2000 security, one of the junior administrators decides to apply the hisec predefined security template on all the servers in your organization. Users start to complain that they cannot access any of the Windows 2000 servers. After a bit of research, you realize that the systems that cannot access the Windows 2000 servers are all non-Windows 2000 systems. How would you make sure that these non-Windows 2000 systems can access the servers again?